PROTEGER A LAS MUJERES Y NIÑAS DE LA VIOLENCIA EN LA ERA DIGITAL

La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

PROTEGER A LAS MUJERES Y NIÑAS DE LA VIOLENCIA EN LA ERA DIGITAL

La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología

Diciembre de 2021

Adriane van der Wilk

Consejo de Europa

Original edition in English:
Protecting women and girls from violence in the digital age - The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women (December 2021)

Violence against Women Division
Council of Europe
F-67075 Strasbourg Cedex
France

Cover design and layout: Documents and Publications Production Department (SPDP), Council of Europe
Photo: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Printed at the Council of Europe

ÍNDICE

RESUMEN EJECUTIVO

Este estudio explora la medida en que dos tratados internacionales, el Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica (Convenio de Estambul) y el Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), pueden contribuir a combatir la violencia contra las mujeres en línea y facilitada por la tecnología mediante políticas coordinadas, prevención, protección, enjuiciamiento y cooperación internacional.

La violencia contra las mujeres en línea y facilitada por la tecnología forma parte del continuo de las diferentes formas de violencia contra las mujeres que tienen lugar fuera de línea. La mayoría de las formas de violencia contra las mujeres en línea y facilitada por la tecnología son crímenes y delitos ya existentes, pero ampliados, amplificados o generalizados por Internet. El impacto en las víctimas y en la sociedad en general es grave; con todo, la impunidad es más bien la regla que la excepción.

El Convenio de Estambul puede ser un instrumento especialmente relevante para abordar la violencia contra las mujeres en línea y facilitada por la tecnología, ya que es el tratado de derechos humanos jurídicamente vinculante de mayor alcance que abarca todas las formas de violencia contra las mujeres y la violencia doméstica. Por su parte, el Convenio de Budapest es el tratado internacional jurídicamente vinculante más relevante en materia de ciberdelincuencia y pruebas electrónicas y, por lo tanto, ofrece la posibilidad de enjuiciar la violencia contra las mujeres en línea y facilitada por la tecnología.

Este estudio establece una categorización y definiciones de las diferentes formas de violencia contra las mujeres en línea y facilitada por la tecnología y hace referencia explícitamente a los artículos 33, 34 y 40 del Convenio de Estambul, complementados por las disposiciones pertinentes del Convenio de Budapest. A continuación, analiza las disposiciones del Convenio de Estambul relativas a las políticas integradas, la prevención, la protección y el enjuiciamiento, y comenta su aplicación en relación con los distintos aspectos del fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología.

Este estudio sostiene que el Convenio de Estambul y el Convenio de Budapest pueden complementarse de manera dinámica: la fuerza del Convenio de Estambul radica en que la violencia contra las mujeres se reconoce como un tipo de violencia que afecta a las mujeres por el hecho de ser mujeres. El Convenio de Budapest aporta medios de gran alcance para la investigación y la obtención de pruebas electrónicas concernientes a los delitos cometidos en línea y facilitados por nuevas tecnologías, así como a todo otro delito que entrañe pruebas electrónicas.

Sin embargo, hasta el día de hoy, el ámbito de la ciberdelincuencia sigue siendo, en gran medida, neutro en lo que al género se refiere, al punto de que los delitos contra las mujeres perpetrados en línea no están conceptualizados en los marcos de lucha contra la ciberdelincuencia, aunque ha habido algunas iniciativas para incorporar la noción de igualdad de género. Debido a su amplio alcance y enfoque integral, el Convenio de Estambul puede ser un instrumento vital para potenciar esos empeños y servir de base para incorporar en el ámbito de la ciberdelincuencia un reconocimiento más sistemático de la exposición de las mujeres a la violencia.

INTRODUCCIÓN

La violencia contra las mujeres y las niñas ha adquirido nuevas dimensiones con el aumento de las tasas de acceso a Internet y el uso más amplio de las tecnologías digitales en todo el mundo. La violencia física, sexual y psicológica que tiene lugar fuera de línea, incluso en la calle, en el hogar o en el lugar de trabajo, resuena, se amplifica, se propaga y se exacerba con las tecnologías de la información y la comunicación (TIC). Asimismo, han surgido nuevas formas de violencia. La violencia contra las mujeres afecta a las mujeres debido a su género y al entrelazamiento de sus identidades; el continuo de la violencia se amplía, resuena y exacerba en línea (Kelly, 1988).

La violencia contra las mujeres en línea y facilitada por la tecnología se produce en diferentes plataformas e implica las más diversas vías, tanto públicas como privadas, como las redes sociales, las aplicaciones de mensajería privada, los correos electrónicos, las aplicaciones de citas, los foros, las secciones de comentarios de los medios de comunicación, los videojuegos o las plataformas de videoconferencia. La violencia suele ser visible para el público y se difunde sin limitaciones constantemente por múltiples medios, proceso que lleva a la victimización repetida de las víctimas. Esas formas de violencia suelen manifestarse en múltiples jurisdicciones, sin consideración de la responsabilidad de los intermediarios ni de los autores de la violencia. Por lo tanto, es difícil comprender el fenómeno y sus consecuencias; los autores de la violencia gozan de aparente impunidad, mientras que las víctimas se sienten indefensas y faltas de apoyo en cada etapa de su victimización. La violencia en línea y facilitada por las nuevas tecnologías tiene graves consecuencias para la vida de las mujeres, su salud física y psicológica y la de las personas a su cargo, sus medios de vida, su reputación, su participación política y su presencia en línea.

A pesar del creciente número de estudios en que se han documentado esos efectos, la inmensa mayoría de los delitos permanecen impunes. Este estudio tiene la finalidad de explorar hasta qué punto dos tratados del Consejo de Europa, el Convenio de Estambul y el Convenio de Budapest, pueden contribuir a combatir la violencia contra las mujeres en línea y facilitada por la tecnología mediante la adopción de políticas, la prevención, la protección, el enjuiciamiento y la cooperación internacional.

El Convenio de Estambul es el primer instrumento jurídicamente vinculante en Europa que ofrece un marco integral para poner fin a la violencia contra las mujeres y la violencia doméstica, y es el instrumento de mayor alcance para combatir la violencia contra las mujeres. Es un texto emblemático de derechos humanos que abarca todas las formas de violencia contra las mujeres. El Convenio reconoce el carácter estructural de la violencia contra las mujeres como violencia de género y reafirma que las mujeres y las niñas corren un mayor riesgo de violencia de género que los hombres. Por consiguiente, el Convenio se aplica a todas las formas de violencia contra las mujeres, incluida la violencia doméstica, y se propone brindarles protección y prevenir, sancionar y eliminar esas formas de violencia, incluida la violencia en el entorno familiar.

Las Partes en el Convenio deberán incorporarlo a su legislación nacional para prevenir la violencia contra las mujeres, brindarles protección y enjuiciar adecuadamente a los autores de esa violencia. El Grupo de Expertos en la lucha contra la violencia contra las mujeres y la violencia doméstica (GREVIO), órgano de expertos independientes encargado de supervisar la aplicación del Convenio de Estambul, y el Comité de las Partes velan por la aplicación efectiva del Convenio, y preparan informes de evaluación, recomendaciones a los Estados Partes y medidas de seguimiento.

El Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest; Consejo de Europa, 2001a) es un tratado jurídicamente vinculante que se centra en la ciberdelincuencia y las pruebas electrónicas. Exige a las Partes la penalización de los delitos perpetrados contra datos y sistemas informáticos, o por medio de ellos, incluidos los delitos relacionados con la producción, difusión o posesión de materiales de abuso sexual de niños y niñas[1] así como las infracciones de los derechos de propiedad intelectual y otros derechos conexos. Asimismo, las Partes en el Convenio deberán establecer facultades y procedimientos para obtener pruebas electrónicas a los efectos de investigaciones penales específicas, no sólo para los delitos mencionados, sino también para todo delito en el que las pruebas estén en forma electrónica. Asimismo, deberán facilitar de manera eficaz la cooperación internacional y la asistencia judicial mutua en relación con la investigación o los procedimientos penales de esos delitos. El Convenio de Budapest se complementa con un Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos a través de sistemas informáticos

1. Al final del documento hay un glosario de términos.

(Consejo de Europa, 2003). El Comité del Convenio sobre la Ciberdelincuencia (T-CY) vela por la aplicación efectiva del Convenio y de su Protocolo adicional.

Los Convenios de Estambul y de Budapest pueden complementarse mutuamente para abordar de forma más eficaz y eficiente la violencia contra las mujeres en línea y facilitada por la tecnología en los Estados Parte. La finalidad de este estudio es analizar y evaluar la protección que ambos instrumentos ofrecen a las víctimas, así como determinar su ámbito de aplicación y su posible complementariedad por lo que se refiere a ciertos tipos de violencia contra las mujeres en línea y facilitada por la tecnología.[2]

En la primera parte de este estudio se define el fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología, se exploran las diferentes formas y características de su victimización y se subrayan las numerosas dificultades a las que se enfrentan las víctimas para obtener reparación. En la segunda parte se presenta el Convenio de Estambul, su alcance y funcionamiento. La tercera parte está dedicada al Convenio de Budapest sobre la Ciberdelincuencia, sus normas conexas y el funcionamiento de su mecanismo de seguimiento. En la cuarta parte se expone el panorama normativo general de los instrumentos internacionales y regionales que abordan, de forma parcial, algunas de esas formas específicas de violencia. La quinta parte se propone categorizar y definir las diferentes formas de violencia contra las mujeres en línea y facilitada por la tecnología en el marco de los artículos 33, 34 y 40 del Convenio de Estambul, complementados, cuando procede, por disposiciones del Convenio de Budapest. En la sexta parte de este estudio se analiza la posibilidad de utilizar, y de qué manera, las normas jurídicas existentes del Convenio de Estambul relativas a integración de políticas, prevención, protección y enjuiciamiento, para combatir la violencia contra las mujeres en línea y facilitada por la tecnología. Asimismo, se analizarán paralelamente disposiciones complementarias del Convenio de Budapest. En la conclusión, se presenta un conjunto de recomendaciones. Este estudio incluye dos anexos en que se analizan formas específicas de violencia, así como un glosario de términos.

En lo que respecta a la violencia contra los niños y las niñas perpetrada en línea y facilitada por las nuevas tecnologías, y a la trata de personas con fines de explotación sexual facilitada por la tecnología, este estudio adoptará el mismo enfoque que el Convenio de Estambul:

> Los redactores decidieron que este Convenio debía evitar abarcar los mismos comportamientos que ya cubren otros convenios del Consejo de Europa, en particular el Convenio sobre la lucha contra la trata de seres humanos (STCE nº 197) y el Convenio para la protección de los niños contra la explotación sexual y el abuso sexual (Convenio de Lanzarote) (STCE nº 201).

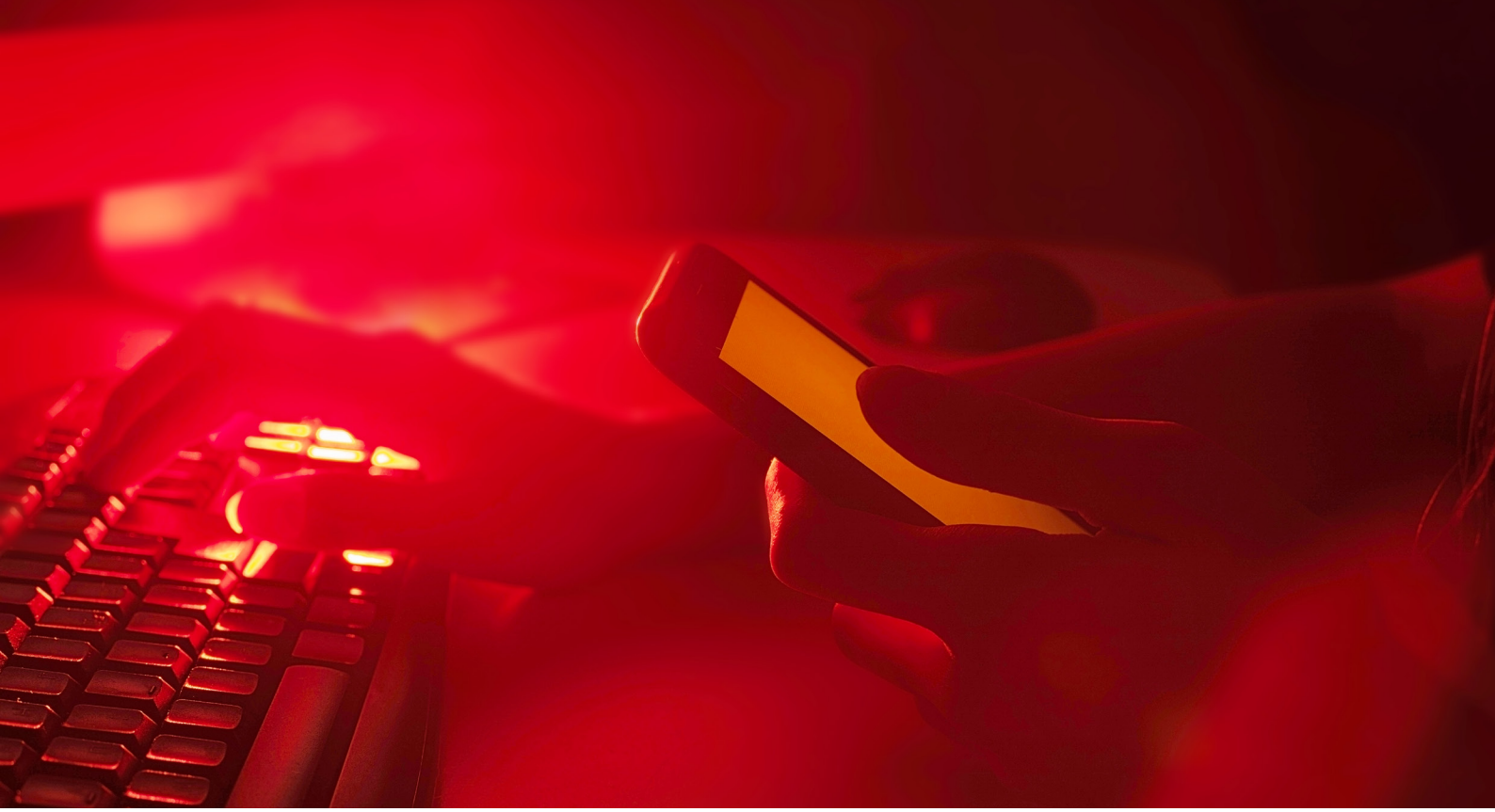
Por consiguiente, este estudio excluirá los tipos de violencia que requieren un enfoque centrado en un solo aspecto. Con todo, son necesarias más investigaciones sobre la interrelación de la violencia contra las mujeres, la explotación y el abuso de niños y niñas en línea y la trata de personas con fines de explotación sexual, tres fenómenos que se han intensificado por las nuevas tecnologías y que en muchos sentidos forman parte del mismo continuo de violencia contra las mujeres y las niñas y las estructuras patriarcales (European Women's Lobby 2017). Entre los más importantes recursos sobre estos temas a nivel del Consejo de Europa cabe destacar la reciente declaración del Presidente del Comité de Lanzarote, "La protección de los niños contra la explotación y el abuso sexual en tiempos de la pandemia de COVID-19" (Consejo de Europa, 2020d); el proyecto "Poner fin a la explotación y el abuso sexual infantil en línea en Europa" (EndOCSEA@Europe) llevado a cabo por la División de Derechos del Niño del Consejo de Europa, en cooperación con la Oficina del Programa de Lucha contra la Ciberdelincuencia del Consejo de Europa (C-PROC), sin olvidar los recursos sobre la dimensión digital de la trata de personas, incluido el "Estudio del Consejo de Europa de 2007 sobre el uso ilícito de Internet para la captación de víctimas de la trata de seres humanos" así como el estudio, de próxima publicación, sobre la trata de seres humanos en línea y facilitada por la tecnología.

Por otra parte, se debe destacar que este estudio se focaliza en las víctimas. Aunque aborda cuestiones cruciales como la protección de datos, la intimidad, la vigilancia, el modelo comercial centrado en la publicidad y la responsabilidad de las empresas de Internet, esas cuestiones interrelacionadas no son el eje central de este trabajo.

En última instancia, el objetivo de este estudio es explicar la manera en que las víctimas de la violencia contra las mujeres en línea y facilitada por la tecnología podrían acogerse a la protección jurídica existente que las Partes de ambos Convenios están obligadas a garantizar a las personas sujetas a su jurisdicción.

---

2. Véase Consejo de Europa 2018c; el estudio sistemático del T-CY sobre la ciberviolencia analiza las respuestas internacionales en el marco del Convenio de Budapest y otros tratados, en particular el Convenio de Estambul.



CAPÍTULO 1.

DEFINICIÓN DE LA VIOLENCIA CONTRA LAS MUJERES EN LÍNEA Y FACILITADA POR LA TECNOLOGÍA

El fenómeno: ¿qué, cómo y dónde?

Definir el fenómeno es crucial para comprender mejor las posibilidades que existen para prevenir todas las formas de violencia contra las mujeres y las niñas, los medios para brindarles mejor protección y la manera de enjuiciar esos tipos de violencia. En esta primera sección, se presentan y analizan varias formas muy específicas de violencia contra las mujeres en línea y facilitada por la tecnología que tienen importantes consecuencias para las víctimas.

La violencia contra las mujeres en línea y facilitada por la tecnología forman parte del continuo de diversas formas de violencia contra las mujeres que ya existían fuera de línea. La mayoría de las formas de violencia contra las mujeres en línea y facilitada por la tecnología son crímenes y delitos ya existentes, que se ven ampliados, amplificados o generalizados por la Internet y las tecnologías digitales, como es el caso de la violencia doméstica:

> El troleo, el abuso verbal, la sextorsión, el intercambio no consentido de imágenes íntimas, la manipulación de fotos, el ciberacoso, el doxeo, la piratería informática, las infracciones de la propiedad intelectual y los ataques DDoS pueden ocurrir exclusivamente en línea, pero también pueden tener lugar en relación con hechos fuera de línea, y casi siempre tienen repercusiones que se experimentan tanto en línea como fuera de línea. (Ging y Siapera, 2018)

Sin embargo, algunas formas también son específicas de las plataformas y herramientas digitales, debido sobre todo a sus efectos, a su permanencia y al número de autores de la violencia involucrados, y "guardan relación con las posibilidades tecnológicas de los nuevos medios de comunicación, las políticas en materia de algoritmos de ciertas plataformas, las culturas del lugar de trabajo que producen esas tecnologías y los individuos y comunidades que las utilizan" (ibíd.).

La violencia contra las mujeres en línea y facilitada por la tecnología tiene lugar en las más diversas plataformas, principalmente en las redes sociales y en sus innumerables características y espacios, pero también en páginas web y foros; motores de búsqueda; aplicaciones de mensajería; blogs; sitios web; aplicaciones de citas; secciones de comentarios en los medios; salas de chat de videojuegos en línea; plataformas de descarga continua (*streaming*); aplicaciones de videojuegos; herramientas de realidad virtual y aumentada; aplicaciones de chat; herramientas de videoconferencia, aplicaciones y sitios web profesionales, etc.

> La violencia facilitada por la tecnología es invasiva y omnipresente; no se limita a un solo ámbito... En cualquier caso, la brecha entre lo público y lo privado, si es que existe, puede verse aún más difuminada y diluida por la tecnología. Debido a la "difuminación de los contextos" entre esas zonas (y las profesionales/personales)... resulta difícil, si no imposible, diferenciar entre el tipo de violencia y el ámbito en el que tiene lugar. (Harris 2020b).

Formas de violencia contra las mujeres facilitada por la tecnología

Las formas de violencia contra las mujeres facilitada por la tecnología incluyen pero no se limitan a las siguientes:

1. El acoso sexual en línea (que incluye el exhibicionismo cibernético [*cyberflashing*], o envío de imágenes sexuales no solicitadas; los comentarios sexualizados; la difamación sexualizada; la suplantación de identidad con fines sexuales; el doxeo [*doxing*]; el troleo [*trolling*] sexualizado y basado en el género, el flameo [*flaming*], los ataques de pandillas [*mob attacks*]; el acoso sexual basado en imágenes, como las fotos rastreras [*creepshots*] (fotos sexualmente sugerentes o íntimas tomadas sin consentimiento y difundidas en línea); las fotos debajo de la falta [*upskirting*] (fotos sexuales o íntimas tomadas debajo de la falda o el vestido sin consentimiento y difundidas en línea); el abuso sexual basado en imágenes (difusión no consentida de imágenes, vídeos o imágenes íntimas; la "pornografía de venganza"; los "ultrafalsos" [*deepfakes*]; las agresiones sexuales y las violaciones grabadas, incluidas las "videoagresiones" [*happy slapping*] transmitidas en vivo o distribuidas en sitios pornográficos; las amenazas y la coerción como el sexteo forzado [*forced sexting*], la sextorsión; las amenazas de violación, y la incitación a cometer una violación.
2. Formas de acoso, vigilancia o espionaje en línea empleando redes sociales o mensajería; robo de contraseñas; descifrado o piratería de dispositivos; instalación de software espía; suplantación de identidad con fines de acoso; geolocalización o localización mediante GPS; intimidación; amenazas, y el control mediante cerraduras inteligentes o electrodomésticos inteligentes.
3. Formas de violencia psicológica como el discurso de odio sexista en línea; la incitación a las autolesiones o al suicidio; las agresiones verbales; los insultos; las amenazas de muerte; las presiones; el chantaje, y el revelar el nombre anterior [*deadnaming*], es decir, emplear en contra de su voluntad el nombre con que fue bautizada una persona trans con el fin de perjudicarla.

Un informe reciente de Plan International sobre la violencia en línea contra las niñas señala que "el tipo más común de ataque es el lenguaje ofensivo e insultante, denunciado por el 59 por ciento de las niñas que han sido objeto de acoso, seguido por la humillación deliberada (41 por ciento), la desvalorización del cuerpo [*body shaming*] y las amenazas de violencia sexual (ambos 39 por ciento)" (Plan International, 2020).

Características de la victimización

Las niñas son un grupo vulnerable y se ven afectadas por formas específicas de violencia infantil en línea y facilitada por la tecnología , con características específicas de género. Es importante señalar que el riesgo es mayor para las mujeres con identidad entrecruzada como las lesbianas, bisexuales, queer y trans, las mujeres de color, las mujeres migrantes, las mujeres que viven con discapacidades o enfermedades crónicas, las mujeres en contextos específicos, como las que viven en situación de violencia doméstica o las mujeres en situación de pobreza. Asimismo, las mujeres que son personajes públicos, como las políticas, las periodistas, las defensoras de los derechos humanos o las activistas están más expuestas a ser objeto de esos tipos de violencia: el 53 por ciento de las periodistas europeas han sido víctimas de ciberacoso según un estudio del Consejo de Europa de 2017 (Consejo de Europa 2017a). En la UE, al menos el 58,2 por ciento de las parlamentarias han sido blanco de ataques sexistas en línea en las redes sociales (IPU, 2018).

En el informe de Plan International citado en el párrafo anterior se señala que:

> Más de un tercio (37 por ciento) de las chicas que pertenecen a una minoría étnica y han sido objeto de abusos dicen que han sido blanco de ataques debido a su raza u origen étnico, mientras que más de la

mitad (56 por ciento) de las que se identifican como LGBTQI dicen que han sido acosadas debido a su identidad de género u orientación sexual.

Varias características constituyen la especificidad de la victimización por esos tipos de violencia de género en línea y facilitada por la tecnología.

1. La primera característica es la relación o ausencia de relación entre la víctima y el agresor, así como el tipo de relación. A guisa de ejemplo, una encuesta británica de 2011 reveló que más de la mitad (54 por ciento) de las encuestadas habían conocido por primera vez en la vida real a su agresor (en línea) (Maple, Shart y Brown 2011). Desde el inicio de la pandemia de Covid-19, a medida que aumenta la interacción en línea de las mujeres, éstas parecen ser objeto de abuso por extraños con mayor frecuencia: una encuesta realizada durante la pandemia por Glitch UK y End Violence Against Women reveló que "el 84 por ciento de las encuestadas experimentaron abuso en línea por parte de desconocidos -- cuentas que no conocían antes del incidente; el 16 por ciento de las encuestadas fueron objeto de abuso por un conocido y el 10 por ciento por una pareja o ex pareja ... El 9 por ciento de las víctimas fueron víctimas de abuso por parte de un compañero o superior en el trabajo" (Glitch y End Violence against Women 2020).
2. La segunda característica es el número de plataformas y de herramientas utilizadas por quienes cometen actos de violencia. La mayoría de las formas de violencia tienen lugar en diferentes tipos de plataformas, tanto públicas como privadas; el ataque puede ocurrir simultáneamente en todas esas plataformas o el autor de la violencia puede valerse de diferentes herramientas. Una víctima puede ser objeto de abuso al mismo tiempo en todas sus redes sociales y plataformas de mensajería; también puede recibir mensajes ofensivos en su correo electrónico, y más tarde ser objeto de ataques fuera de línea, por teléfono o por parte de agresores reales en su domicilio, en el trabajo, etc. La reciente ley francesa contra la violencia sexual y sexista tiene en cuenta, por ejemplo, el hecho de que los "ataques de pandillas" [*mob attacks*] son un comportamiento típico; la ley tiene en cuenta el aspecto repetitivo del acoso, la multiplicidad de lugares y el hecho de que varios agresores pueden acosar a la misma víctima simultáneamente (Legifrance, 2018).
3. De hecho, la tercera característica de esos tipos de violencia es el número de agresores y el perfil de los mismos. Ciertos tipos de violencia contra las mujeres en línea y facilitada por la tecnología son realizados simultáneamente por varios agresores, como es el caso de los ataques de pandillas, la intimidación en línea (en el caso de los niños y las niñas) o el acoso sexual por parte de todo un grupo o comunidad.[3] La difusión no consentida de imágenes también es propiciada por docenas, cientos o a veces miles de personas. El comportamiento denominado "mentalidad de pandilla" es una característica de las redes sociales: los agresores se ocultan tras perfiles anónimos, tienen una sensación de impunidad, se sienten apoyados por su comunidad o, cuando no ocultan su nombre real, no relacionan la persona atacada con una persona real. El diseño de algoritmos permite la formación de pandillas, ya que los algoritmos favorecen ante todo la participación y el incremento del número de miembros. A pesar de los esfuerzos por identificar el lenguaje ofensivo y el contenido visual, los algoritmos promueven la visibilidad de los contenidos, que pueden ser brutales e incluso violentos, lo que facilita la polarización. Además, "esto puede verse amplificado por características que enlazan contenidos abusivos, como ocurre con las etiquetas (*hashtags*) que conectan diferentes casos de misoginia dando lugar a una campaña" (Harris y Megarry, 2014). Zarizana Abdul Aziz, directora del *Due Diligence Project*, establece una distinción entre agresores primarios y agresores secundarios. El agresor primario es quien origina y sube el contenido abusivo mientras los agresores secundarios lo difunden (Abdul Aziz, 2017).
4. La cuarta característica de la violencia contra las mujeres en línea y facilitada por la tecnología es la incidencia de la violencia en línea. ¿Cuánto tiempo duró el abuso, con qué frecuencia ocurrió, cuán permanentes son los datos perjudiciales? En la mayoría de los casos de abuso basados en imágenes siempre existe la posibilidad de que la víctima vuelva a ser victimizada repetidamente, ya que las imágenes han sido difundidas en línea por miles de cuentas en todas partes. De hecho, las formas típicas de violencia en línea incluyen un aspecto repetitivo y la permanencia de los contenidos dañinos.
5. Debido a su incidencia y permanencia, las repercusiones para la vida de las víctimas son considerables. La magnitud de la violencia puede marcar a las víctimas de por vida. Esas formas de violencia tienen consecuencias negativas para sus familias, sus hijos e hijas, sus empleos, sus relaciones, su salud mental

3. Véase, por ejemplo, el *GamerGate*, una campaña de acoso en línea contra una diseñadora de videojuegos que incluía doxeo, difusión no consentida de imágenes íntimas, violación y amenazas de muerte.

y física y, en definitiva, su esperanza de vida. Un reciente estudio de la UE sobre este fenómeno estima que el coste anual global del ciberacoso contra las mujeres oscila entre 49.000 y 89.300 millones de euros, incluidos los costes de la atención médica, los costes jurídicos, los costes del mercado laboral y los costes asociados a una menor calidad de vida (Servicio de Estudios del Parlamento Europeo, 2021).

Dificultades a las que se enfrentan las víctimas

Por otra parte, las víctimas experimentan diferentes tipos de dificultades para obtener reparación.

1. A menudo resulta difícil identificar el tipo de violencia, ya que la mayoría de las formas de violencia en línea no tienen una definición jurídica clara y muchas formas se traslapan. La mayoría de las plataformas de redes sociales ofrecen a sus usuarios definiciones muy limitadas, casi nunca hacen mención a las leyes, y la información relativa a la denuncia de abusos puede ser limitada e incompleta. Además, las páginas en que el usuario puede presentar denuncias suelen carecer de una perspectiva interseccional sobre los tipos de violencia.
2. Documentar la violencia es un elemento crucial; con todo, la mayoría de las víctimas desconocen que tienen la posibilidad y, en la mayoría de los casos, la responsabilidad de conservar el contenido ofensivo (si estuviera disponible), para poder presentar cargos. De hecho, las pruebas pueden desaparecer, ser borradas por los agresores o no ser del conocimiento de la víctima. Por otra parte, las pruebas contra los agresores pueden estar almacenadas en la nube, en otros países o en dispositivos privados desconectados. Reunir el mayor número posible de pruebas de los abusos puede facilitar su enjuiciamiento.
3. Por lo general, las mujeres víctimas de violencia de género enfrentan muchas dificultades para presentar denuncias. En los casos de violencia contra las mujeres en línea y facilitada por la tecnología, en muchos países resulta difícil lograr presentar su queja ante agentes de la ley capacitados que den crédito a su denuncia. Incluso cuando ello es posible en ciertas localidades de un país, puede seguir siendo bien difícil en zonas más remotas. La mayoría de los agentes del orden no han recibido formación para reconocer los diferentes tipos de violencia en línea que afectan a las mujeres y las niñas, y muchos de ellos no saben cómo proceder en esos casos. Esa falta de formación reduce las posibilidades de las mujeres para presentar denuncias de manera eficaz. Además, durante la tramitación de las denuncias, la culpabilización de las víctimas suele ser algo omnipresente. Para citar a una abogada: "No cabe esperar que un policía típico de la comisaría de tu barrio pueda atender a las 11 de la noche una denuncia por abuso sexual basado en imágenes".[4] Por otra parte, puede ocurrir que solo ciertos cuerpos de policía estén facultados para investigar tales delitos, por lo que las víctimas podrían simplemente desconocer a qué unidad deben dirigirse para presentar la denuncia (Consejo de Europa, 2018c).
4. Este tipo de casos supone un ingente trabajo de investigación. "Hay un elevado número de denuncias y mensajes; la identificación de las personas puede tomar mucho tiempo: la solicitud de información a los proveedores de servicios consume muchos recursos. Cuando se trata de un único agresor la situación es sencilla, pero imagínense lo que ocurre si se trata de 500, o incluso de 3.000. Hay que pedir información a los proveedores de servicios sobre cada uno de ellos. De no haber un investigador comprometido e interesado en el caso, nadie hará ese trabajo y este tipo de casos guardan relación con una investigación preliminar".[5] Por otra parte, las pruebas del delito se almacenan cada vez más en servidores situados en jurisdicciones extranjeras múltiples, variables o desconocidas, es decir, en la nube, por lo que las competencias de las fuerzas policiales están limitadas por las fronteras territoriales. Por consiguiente, la cooperación internacional es primordial.
5. A día de hoy, son contadas las leyes que abarcan de forma exhaustiva todos los tipos de abusos de que son objeto las mujeres en línea. Las sanciones, cuando se aplican, pudieran no reflejar los efectos de la violencia en la vida de la víctima, ni el componente de género de un delito que tiene lugar en línea o facilitada por la tecnología. La Secretaría del Convenio de Budapest ha calculado que sólo el 1 por ciento de los ciberdelitos se denuncian a las fuerzas del orden y que menos del 1 por ciento de las denuncias conduce realmente a un resultado de justicia penal. Por lo tanto, de hecho se imponen sanciones solo en un número muy reducido de casos de ciberdelincuencia.[6]

4. Entrevista con Maïtre Frety, abogado, septiembre de 2020, traducida por la autora, www.frety-avocats.fr/.
5. *Ibíd.*
6. Entrevista con Alexander Seger, Jefe de la División de Ciberdelincuencia y Secretario Ejecutivo del Comité del Convenio sobre Ciberdelincuencia, septiembre de 2020.

6. La dimensión transversal de la culpabilización de las víctimas y la normalización de la violencia en los medios de comunicación y en la sociedad en general, que influye en la comprensión y criminalización de todas las formas de violencia de género contra las mujeres, también está presente en los casos de violencia contra las mujeres en línea y facilitada por la tecnología: "Sin programas de apoyo y educación sobre la culpabilización de las víctimas, las víctimas de pornografía de venganza pueden experimentar niveles elevados de problemas emocionales al tratar de hacer frente a la situación. Incluso cuando han presentado su denuncia a la policía, algunas víctimas de la pornografía de venganza han informado que los agentes les han echado la culpa a ellas y que les han negado asistencia ya que los policías opinaban que la víctima era la culpable del incidente (Citron y Franks, 2014; Wolak y Finkelhor, 2016). Algo similar ocurre con las víctimas de violación, a las que a veces se reprocha su victimización a pesar de la formación que reciben los agentes de policía especializados (Sleath y Bull, 2012). Por lo tanto, por lo que se refiere al creciente delito de la pornografía de venganza es importante tener en cuenta el papel de la culpabilización de las víctimas" (Tegan, Starr y Lavis, 2018).

CAPÍTULO 2.

EL CONVENIO DE ESTAMBUL Y LA VIOLENCIA CONTRA LAS MUJERES EN LÍNEA Y FACILITADA POR LA TECNOLOGÍA

El Convenio de Estambul y su Informe explicativo fueron adoptados por el Comité de Ministros del Consejo de Europa el 7 de abril de 2011. El Convenio se abrió a la firma el 11 de mayo de 2011 con motivo de la 121ª Sesión del Comité de Ministros en Estambul. Entró en vigor el 1 de agosto de 2014 y, en octubre de 2021, treinta y cuatro Estados eran Partes en el Convenio. El Convenio está abierto a la adhesión de cualquier país que esté dispuesto a aplicar sus disposiciones.

El Convenio de Estambul, tratado emblemático en materia de derechos de la mujer, consagra el conjunto más completo de medidas que permiten a los gobiernos prevenir y combatir todas las formas de violencia contra la mujer y la violencia doméstica. Plantea que esa violencia es una violación de los derechos humanos y una forma de discriminación contra la mujer y vincula firmemente su erradicación con el logro de la igualdad entre hombres y mujeres. En su preámbulo (Consejo de Europa 2011a), el Convenio recuerda el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, la Carta Social Europea y el Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos, así como el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual. Asimismo, el Convenio de Estambul evoca la Convención de las Naciones Unidas sobre la eliminación de todas las formas de discriminación contra la mujer (CEDAW) y sus posteriores recomendaciones generales, la Convención de las Naciones Unidas sobre los Derechos del Niño y la Convención de las Naciones Unidas sobre los Derechos de las Personas con Discapacidad.

El texto reafirma la naturaleza estructural y de género de la violencia contra las mujeres y propone un marco integral para poner fin a la violencia contra las mujeres y la violencia doméstica. El convenio se estructura en torno a las "4 P": prevención; protección y apoyo a las víctimas; persecución de los agresores, y políticas coordinadas (Consejo de Europa, 2020c).

Ámbito de aplicación

En cuanto a su ámbito de aplicación (artículo 2) (Consejo de Europa, 2011a), el Convenio de Estambul "se aplicará a todas las formas de violencia contra las mujeres, incluida la violencia doméstica" y "se aplicará en tiempos de paz y en situaciones de conflicto armado", abarcando todas las situaciones en las que las mujeres son objeto de violencia.

El Convenio establece una serie de definiciones y conceptos y define la violencia contra las mujeres como "una violación de los derechos humanos y una forma de discriminación contra las mujeres" y una forma de actos de violencia basados en el género "que implican o pueden implicar para las mujeres daños o sufrimientos de naturaleza física, sexual, psicológica o económica" (artículo 3a), dirigidos contra la mujer en razón de su género y por los "los papeles, comportamientos, actividades y atribuciones socialmente construidos" (artículo 3c).

Además, el artículo 3a también establece que "las amenazas de realizar dichos actos, la coacción o la privación arbitraria de libertad, en la vida pública o privada" se consideran "violencia contra las mujeres por razones de género". El término "mujer" incluye a las niñas menores de 18 años (artículo 3f).

En el artículo 4, el Convenio estipula que "Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para promover y proteger el derecho de todos, en particular de las mujeres, a vivir a salvo de la violencia tanto en el ámbito público como en el ámbito privado". En el artículo 5, el Convenio integra las normas de diligencia debida exigidas a las Partes: "Las Partes tomarán las medidas legislativas y otras necesarias para actuar con la diligencia debida para prevenir, investigar, castigar y conceder una indemnización por los actos de violencia incluidos en el ámbito de aplicación del presente Convenio cometidos por actores no estatales", recordando así a las Partes en el Convenio que tienen la obligación de elaborar políticas integradas para prevenir, proteger y perseguir todas las formas de violencia que afecten a las mujeres y las niñas, tanto en la vida pública como en la privada.

> Este principio no impone una obligación de resultado, sino una obligación de medios. Se pide a las Partes que organicen su respuesta a todas las formas de violencia contempladas en este Convenio de manera que las autoridades competentes puedan prevenir dichos actos de violencia o realizar investigaciones, sancionar a los agresores y conceder reparaciones por dichos actos de violencia. El incumplimiento de esta obligación compromete la responsabilidad del Estado por un acto que, de otro modo, sólo sería atribuible a un agente no estatal. (Consejo de Europa, 2011b)

El Convenio aspira a poner coto a las actitudes que condonan la violencia contra las mujeres y las niñas, o contribuyen a perpetuarla. Incluye obligaciones precisas para dar pasos encaminados a prevenir todas las formas de violencia contra las mujeres mediante la sensibilización y la educación, incluida la formación de profesionales y la labor con los agresores. Las medidas de protección y apoyo a las víctimas y a las personas en situación de riesgo deberán ser comprensibles para todos, centrarse en las víctimas, e ir dirigidas a lograr su empoderamiento. Deberán llevarse a cabo investigaciones e incoarse procedimientos penales con el fin de llevar ante la justicia a los agresores y garantizar que rindan cuenta de sus actos. Todo lo anterior debe formar parte de una respuesta integral a las diferentes formas de violencia contra las mujeres, característica que destaca el carácter singular de este importante tratado jurídico.

Aunque el Convenio de Estambul no contiene una referencia explícita a la dimensión digital de la violencia contra las mujeres, su ámbito de aplicación, tal como se define en el artículo 2, abarca la violencia cometida en el espacio digital, como lo previeron sus redactores. De hecho, varios artículos del Convenio de Estambul son aplicables en el contexto digital y se abordan en detalle en este estudio. Por ejemplo, el artículo 40 es aplicable al acoso sexual en línea y facilitado por la tecnología con arreglo a su definición: "toda forma de comportamiento no deseado, verbal, no verbal o físico, de carácter sexual, que tenga por objeto o resultado violar la dignidad de una persona, en particular cuando dicho comportamiento cree un ambiente intimidatorio, hostil, degradante, humillante u ofensivo".

La disposición del Convenio en materia de acoso (artículo 34) también se aplica al acoso en línea y facilitado por la tecnología, ya que en ese documento el acoso se define como "el hecho, cuando se cometa intencionadamente, de adoptar en varias ocasiones un comportamiento amenazador contra otra persona, que lleve a ésta a temer por su seguridad". La ampliación del ámbito de aplicación del artículo 34 a la esfera digital se ha confirmado en el Informe explicativo del Convenio (ibíd.), que clasifica explícitamente como contacto no deseado en el sentido de dicha disposición "la búsqueda de cualquier contacto activo con la víctima a través de cualquier medio de comunicación disponible, incluidas las herramientas modernas de comunicación y las TIC". En vista de las graves consecuencias psicológicas que muchas formas de violencia en línea y facilitada por la tecnología pueden tener para las mujeres y las niñas, el requisito del Convenio de Estambul de tipificar como delito la violencia psicológica (artículo 33) reviste un sentido importante.

Mecanismos de seguimiento

Dos órganos de seguimiento distintos, pero interrelacionados, garantizan el seguimiento del Convenio de Estambul.

El Grupo de Expertos en la lucha contra la violencia contra las mujeres y la violencia doméstica (GREVIO), órgano de expertos independientes, vela por la aplicación del Convenio. En la actualidad, el GREVIO cuenta con 15 expertos que poseen conocimientos multidisciplinarios "en materia de derechos humanos, igualdad entre mujeres y hombres, violencia contra la mujer y violencia doméstica o en asistencia y protección a las víctimas". El GREVIO lleva a cabo procedimientos de evaluación en los distintos países y supervisa la aplicación efectiva del Convenio de Estambul en los Estados Partes.[7] Esos procedimientos de evaluación país por país se traducen en orientaciones específicas para cada país destinadas a potenciar el nivel de aplicación e incluyen una evaluación de referencia de las medidas adoptadas para dar sentido a todas las obligaciones del Convenio. Los informes de evaluación de referencia del GREVIO, incluidos los comentarios de la Parte, se hacen públicos.[8] El GREVIO cumple una función única

> En el seguimiento de la aplicación de un instrumento tan exhaustivo... El GREVIO se considera una plataforma de referencia y se espera que genere datos inestimables derivados de su análisis en profundidad de la normativa legal nacional e internacional respecto de la violencia contra las mujeres. Asimismo, se espera que facilite el intercambio de buenas prácticas entre los Estados en relación con los empeños orientados a erradicar la violencia contra las mujeres (Guney, 2020).

El Comité de las Partes es el órgano político encargado de supervisar la aplicación del Convenio. La función del Comité se describe en el artículo 67 del Convenio. Está integrado por representantes de las Partes en el Convenio.

Sobre la base de los informes elaborados por el GREVIO, el Comité de las Partes adopta recomendaciones en las que se destacan las medidas que deben adoptarse "para aplicar las conclusiones del GREVIO,... destinadas a promover la cooperación con esa Parte para la correcta aplicación del Convenio" (Consejo de Europa, 2015a). El Comité supervisa la aplicación de esas recomendaciones al cabo de un período de tres años.

En el marco de su procedimiento de evaluación de referencia, el GREVIO ha venido aplicando los artículos mencionados del Convenio de Estambul en el contexto digital y supervisado su aplicación en relación con determinados aspectos de la violencia en línea y facilitada por la tecnología, incluidos el ciberacoso y el acoso sexual en línea. En sus informes de evaluación de referencia, el GREVIO ha destacado las buenas prácticas de los Estados Parte. Por ejemplo, en el informe de evaluación sobre Francia se elogió la incorporación de nuevos delitos penales en el sistema jurídico francés, incluido el ciberacoso contra mujeres y niñas. Asimismo, el GREVIO elogió las enmiendas introducidas en los códigos penales de Eslovenia y Polonia, que amplían el alcance de los delitos de acoso para incluir sus manifestaciones en línea. En su procedimiento de evaluación de referencia, el GREVIO también examinó las prácticas educativas de los Estados Parte en el Convenio de Estambul: en Portugal se acogió con satisfacción la adopción de un conjunto completo de guías sobre género y ciudadanía, que incluyen directrices sobre la seguridad en Internet, en todos los niveles de educación, desde la enseñanza preescolar hasta la secundaria. Los esfuerzos de Mónaco por prevenir el ciberacoso en todas las clases, desde el sexto al décimo año, fueron bien recibidos en la evaluación del país por parte del GREVIO. Asimismo, se tomó nota con satisfacción de los esfuerzos de Eslovenia destinados a sensibilizar a los jóvenes acerca de la violencia en las citas, incluida su dimensión en línea, y a mejorar los conocimientos y la sensibilidad de los profesionales pertinentes, incluidos los maestros y los trabajadores sociales, para proteger a niñas y mujeres y prevenir eficazmente la violencia y el acoso en línea.

Además de destacar las buenas prácticas, los informes de evaluación de referencia del GREVIO también llaman la atención sobre los aspectos a que deben prestar mayor atención los Estados miembros. Por ejemplo, en el informe de evaluación de referencia sobre Francia se pedía que se llevaran a cabo actividades de sensibilización y promoción en relación con la ciberviolencia verbal y sexual contra las niñas. Asimismo, en el informe de evaluación de referencia correspondiente a los Países Bajos se señaló la falta de formación de los profesionales acerca de la dimensión digital de la violencia contra las mujeres. A su vez, en el informe de España se alentó

7. Los informes están disponibles en: www.coe.int/en/web/istanbul-convention/country-monitoring-work
8. Para más información sobre los mecanismos de seguimiento del Convenio de Estambul véase: www.coe.int/en/web/istanbul-convention/about-monitoring1

a las autoridades a que intensificaran las actividades de formación de grupos profesionales como los agentes del orden, los maestros, las enfermeras y otros profesionales de la salud sobre las diversas formas de violencia contra las mujeres, incluida su dimensión digital.

El GREVIO ha elogiado la adopción de leyes nacionales que abordan la dimensión digital de la violencia contra las mujeres, pero también ha identificado las deficiencias comunes que imperan en la mayoría de los países. Por ejemplo, las sanciones suelen centrarse en garantizar la seguridad, la reputación o la propiedad de una persona; sin embargo, no prestan la debida atención a otras consecuencias de ese tipo de violencia, incluidos los perjuicios sociales, económicos y psicológicos, ni a los efectos sobre la participación. Y lo que es aún más importante: la mayoría de las leyes nacionales no contemplan todavía la violencia contra las mujeres cometida por medios digitales dentro del continuo de formas de violencia que afectan a mujeres y niñas en todos los ámbitos de la vida.

La primera recomendación general adoptada por el GREVIO en octubre de 2021 respecto del artículo 69 del Convenio de Estambul aclara aún más la aplicación de ese Convenio en lo que se refiere a las expresiones digitales de la violencia contra las mujeres. Propone una interpretación exhaustiva del Convenio en el contexto de la violencia en línea y facilitada por la tecnología; aclara, en términos prácticos, las obligaciones de los Estados miembros al respecto y hace recomendaciones concretas. Al igual que la violencia contra las mujeres cometida fuera de línea, la dimensión digital de la violencia contra las mujeres es muy compleja y pluridimensional. La recomendación general presenta un enfoque integral y multisectorial para abordar el problema en relación con los cuatro pilares ("las 4 P") del Convenio de Estambul.

Relación con otros instrumentos

El Convenio de Estambul también evalúa y explica la relación del Convenio con otros instrumentos existentes y futuros, tanto nacionales como internacionales, en el Capítulo X, Relación con otros instrumentos internacionales (Consejo de Europa 2011b).

> En el Informe explicativo del Convenio se subraya que el Convenio coexiste armoniosamente con otros tratados, tanto multilaterales como bilaterales... El objetivo principal del Convenio es potenciar la protección de las víctimas garantizándoles el mayor grado de protección posible... Es importante destacar "el mayor grado de protección". Se puede sostener que deberá prevalecer el criterio que brinde el mayor grado de protección, trátese del Convenio de Estambul o de cualquier otro instrumento. Ello está en consonancia con el enfoque centrado en las víctimas adoptado en el Convenio de Estambul, en el que se da prioridad al interés superior de las víctimas. (Guney, 2020)

De hecho, el artículo 71 subraya que "el presente Convenio no afectará a las obligaciones derivadas de otros instrumentos internacionales en los que las Partes en el presente Convenio sean o serán Partes y que contengan disposiciones relativas a las materias que abarca el presente Convenio", lo que recuerda a las Partes que también siguen teniendo las obligaciones establecidas en otros tratados sobre derechos de la mujer que hayan ratificado o que puedan ratificar en el futuro.

El artículo 73 añade que "las disposiciones del presente Convenio no afectarán a las disposiciones de la legislación interna ni a las de otros instrumentos internacionales vinculantes vigentes o que puedan entrar en vigor y en cuya aplicación se reconozcan o puedan ser reconocidos a las personas derechos más favorables en materia de prevención y de lucha contra la violencia contra las mujeres y la violencia doméstica", lo que reconoce que otros instrumentos podrían garantizar mayor protección a las víctimas de la violencia de género contra las mujeres y complementar así el Convenio de Estambul. Además, el artículo 72 estipula que otros acuerdos concertados sobre la cuestión de la protección de las mujeres contra la violencia, tanto bilaterales como multilaterales, pueden servir para complementar o reforzar el Convenio de Estambul.

En la siguiente parte de este estudio se presentará el Convenio de Budapest y sus características específicas y se examinarán concretamente otros instrumentos existentes además del Convenio de Estambul y su cobertura de algunos tipos de violencia contra las mujeres en línea y facilitada por la tecnología.

CAPÍTULO 3.
EL CONVENIO DE BUDAPEST

El texto y su ámbito de aplicación

El Convenio del Consejo de Europa sobre la Ciberdelincuencia (el Convenio de Budapest) es el primer y más importante tratado internacional jurídicamente vinculante que se centra en la ciberdelincuencia y las pruebas electrónicas.

El Convenio y su Informe explicativo fueron adoptados por el Comité de Ministros del Consejo de Europa en noviembre de 2001. Se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004. En junio de 2021, 66 Estados eran Parte en el Convenio. El Convenio está abierto a la adhesión de cualquier país dispuesto a aplicar las disposiciones de ese tratado y a participar en la cooperación internacional en la lucha contra la ciberdelincuencia. Es importante destacar que sirve de guía para cualquier país que elabore una legislación nacional integral contra la ciberdelincuencia y todos los delitos que entrañen pruebas electrónicas; gran número de Estados ya se han acogido al mismo.[9]

El Convenio exige a las Partes la penalización de los delitos perpetrados contra datos y sistemas informáticos o por medio de ellos; de los delitos relacionados con el contenido concernientes a la producción, difusión o posesión de materiales de abuso sexual de niños y niñas; y de las infracciones de los derechos de propiedad intelectual. Asimismo, las Partes en el Convenio deberán reforzar sus competencias en cuanto al derecho procesal penal interno y dotar a su sistema judicial de los medios necesarios para obtener pruebas electrónicas en relación con cualquier delito. Las Partes deberán también facilitar eficazmente la cooperación internacional y la asistencia judicial mutua en lo que respecta a la investigación y el enjuiciamiento de la ciberdelincuencia y otros delitos que entrañan pruebas electrónicas. Los objetivos principales del Convenio son: 1) armonizar los elementos del derecho penal sustantivo nacional respecto de los delitos y las disposiciones conexas en el ámbito de la ciberdelincuencia; 2) establecer los poderes y procedimientos del derecho procesal nacional que sean necesarios para la investigación y el enjuiciamiento de dichos delitos, así como de otros delitos en que se

9. Consejo de Europa, "The global state of cybercrime legislation 2013-2020: A cursory overview", disponible en: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9.

emplee un sistema informático o en que las pruebas de esos delitos estén en formato electrónico; 3) establecer un régimen rápido y eficaz de cooperación internacional (Consejo de Europa, 2001a).

El éxito y la legitimidad del Convenio de Budapest se deben, en muchos sentidos, a que las medidas previstas permiten conciliar una respuesta eficaz de la justicia penal con las garantías del estado de derecho.

Protocolos adicionales al Convenio de Budapest

El primer Protocolo Adicional

El Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos fue adoptado por el Comité de Ministros del Consejo de Europa en noviembre de 2002 y entró en vigor el 1 de marzo de 2006. En junio de 2021, 33 Estados eran Parte en el Protocolo Adicional.

El Protocolo reconoce que los sistemas informáticos facilitan la comunicación y la libertad de expresión, pero también la difusión de materiales racistas y xenófobos, y exige a las Partes la tipificación penal de la difusión de esos materiales.

El Protocolo se centra en la difusión de material racista y xenófobo mediante sistemas informáticos, las amenazas e insultos de carácter racista y xenófobo y la negación, la minimización burda y la aprobación o justificación del genocidio o de los crímenes contra la humanidad.

El Protocolo supone una ampliación del ámbito de aplicación del Convenio, incluidas sus disposiciones sustantivas, de procedimiento y de cooperación internacional, para abarcar también los delitos de propaganda racista y xenófoba. Por tanto, además de armonizar los elementos de derecho sustantivo de tales conductas, el Protocolo tiene por objeto potenciar la capacidad de las Partes para hacer uso de los medios y vías de cooperación internacional establecidos en el Convenio en esa esfera (Consejo de Europa, 2003).

El próximo Segundo Protocolo Adicional

En septiembre de 2017 comenzó la preparación de un Segundo Protocolo Adicional al Convenio de Budapest, que abordará los problemas relativos a la justicia penal en el ciberespacio y establecerá una cooperación más eficaz en materia de ciberdelincuencia y pruebas electrónicas. Las pruebas electrónicas revisten suma importancia para la investigación no solo de los delitos cibernéticos, sino también de todo otro tipo de delito. Las competencias de las autoridades de justicia penal se ven limitadas por las fronteras territoriales; sin embargo, los agresores, las víctimas y las pruebas electrónicas pueden encontrarse en múltiples jurisdicciones y, en muchos casos, no está claro qué leyes se aplican ni la manera de obtener esas pruebas.

Esto tiene efectos negativos para el estado de derecho y las obligaciones de los gobiernos de proteger a las personas en el ciberespacio. Al igual que ocurre con el Convenio de Budapest, las medidas del Protocolo están concebidas únicamente para investigaciones penales específicas y están sujetas al respeto del estado de derecho y a las salvaguardias de la protección de datos.

Está previsto que el Segundo Protocolo Adicional se adopte y se abra a la firma a fines de 2021.

Ese instrumento tiene por objeto facilitar la cooperación en lo que se refiere a la ciberdelincuencia y la obtención de pruebas electrónicas mediante la adopción de instrumentos adicionales que promoverán una asistencia mutua más eficaz y nuevas formas de cooperación entre las autoridades competentes. Asimismo, se fortalecerá la cooperación en situaciones de emergencia, es decir, en situaciones en las que exista un riesgo significativo e inminente para la vida o la seguridad de cualquier persona física. Por otra parte, se reforzará la cooperación directa entre las autoridades competentes y los proveedores de servicios y otras entidades que posean o controlen la información pertinente para la identificación de los delincuentes.[10]

Por consiguiente, el Segundo Protocolo vendrá a complementar el Convenio y el Primer Protocolo Adicional. Sus disposiciones serán útiles desde el punto de vista operativo y político y garantizarán la pertinencia constante del Convenio de Budapest.

10. Comité del Convenio sobre la Ciberdelincuencia (T-CY) (2020), "Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, State of play", disponible en: https://rm.coe.int/t-cy-2020-32-protocol-tor-chair-state-of-play/1680a06a83%20or%20just%20a%20general%20page:%20Protocol%20negotiations%20(coe.int)www.coe.int/en/web/cybercrime/t-cy-drafting-group.

Comité de Seguimiento y Oficina del Programa contra la Ciberdelincuencia

El Comité del Convenio sobre la Ciberdelincuencia (T-CY) vela por la aplicación efectiva del Convenio de Budapest y representa a los Estados Parte en el mismo.

El artículo 46 del Convenio de Budapest define las funciones del Comité. El T-CY facilita el uso y la aplicación efectivos del Convenio. Además, el Comité facilita el intercambio de información pertinente entre las Partes en el ámbito de la ciberdelincuencia y la obtención de pruebas en formato electrónico. Por último, el T-CY también es responsable de preparar las posibles enmiendas al Convenio.[11]

Como complemento a la labor del T-CY se ha creado la Oficina del Programa de Lucha contra la Ciberdelincuencia del Consejo de Europa (C-PROC) en Bucarest, Rumanía. La tarea de C-PROC es dotar a los países de todo el mundo de los medios necesarios para fortalecer sus sistemas judiciales y jurídicos para que puedan hacer frente de manera eficaz a la ciberdelincuencia y a los delitos que entrañan pruebas electrónicas, tanto a nivel nacional como internacional. C-PROC se centra específicamente en asesorar a los Estados en la redacción de nuevas leyes, o en su actualización, sobre la base del Convenio de Budapest y las normas conexas. Asimismo, brinda asistencia destinada a fortalecer la capacidad de la justicia penal para responder a los desafíos planteados por la ciberdelincuencia y las pruebas electrónicas y para mejorar la cooperación internacional, interinstitucional y entre los sectores público y privado. Si bien el Consejo de Europa puede apoyar a cualquier país en el fortalecimiento de su legislación nacional en materia de ciberdelincuencia, la adhesión de un gobierno al Convenio de Budapest representa un compromiso político y permite brindar todo tipo de asistencia para reforzar las capacidades de la justicia penal. C-PROC obra también para proteger a los niños y las niñas contra la violencia sexual en línea y, a través de una serie de actividades sobre la violencia cibernética, explora las sinergias entre el Convenio de Estambul y el Convenio de Budapest, y otros instrumentos.[12] El desarrollo de capacidad ha demostrado ser eficaz para ayudar a las sociedades a afrontar el creciente reto planteado por la ciberdelincuencia y las pruebas electrónicas, incluso en relación con la investigación, el enjuiciamiento y las sanciones de la violencia contra las mujeres en línea y facilitada por la tecnología.

Por consiguiente, el Convenio de Budapest y sus protocolos adicionales, tanto el actual como el futuro, representan un marco muy interesante para reflexionar sobre el fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología, en relación con el Convenio de Estambul. El Convenio de Budapest, mediante una serie de disposiciones de Derecho penal sustantivo, aborda directa e indirectamente algunos tipos de violencia contra las mujeres en línea y facilitada por la tecnología. Otras disposiciones abordan los actos que facilitan ese tipo de violencia. Las competencias procesales y las disposiciones en materia de cooperación internacional del Convenio sobre la Ciberdelincuencia revisten interés para la investigación de los actos de violencia contra las mujeres en línea y facilitada por la tecnología y para la obtención de pruebas electrónicas.

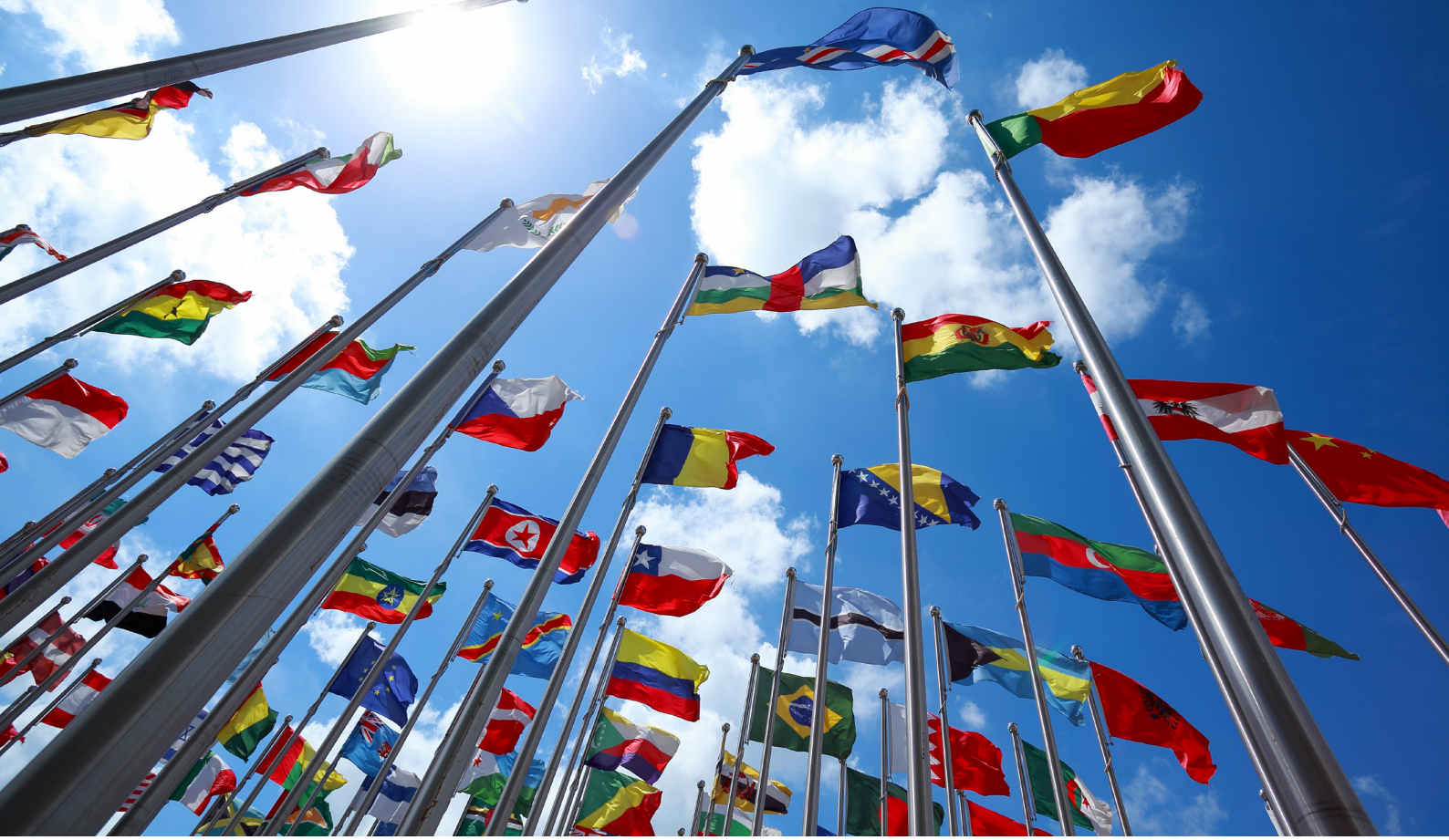
En los dos capítulos anteriores se ha señalado que el ámbito de aplicación del Convenio de Estambul abarca todas las formas de violencia contra las mujeres, que reafirma el carácter estructural y de género de la violencia contra las mujeres y que el Convenio está estructurado en torno a la prevención, la protección y el apoyo a las víctimas, el enjuiciamiento de los delincuentes y el desarrollo de políticas coordinadas. Se ha destacado también que las Partes están obligadas a ofrecer la debida diligencia a sus ciudadanos en relación con esos cuatro pilares.

También hemos visto que el Convenio sobre la Ciberdelincuencia del Consejo de Europa abarca los delitos penales perpetrados por medio de ordenadores; por otra parte, las disposiciones procesales y de cooperación internacional se aplican a cualquier delito que implique pruebas electrónicas, lo que complementa las disposiciones del Convenio de Estambul relativas a la cuestión específica de la violencia contra las mujeres en línea y facilitada por la tecnología y, por lo tanto, facilita la investigación de ese tipo de violencia.

Existen muchos otros instrumentos internacionales que abarcan partes del fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología. El Convenio de Estambul reconoce que, en relación con algunas cuestiones específicas, otros instrumentos jurídicos pueden ofrecer un mayor grado de protección, y afirma expresamente que tendrán prioridad. Con todo, esos instrumentos no coinciden necesariamente para responder al creciente fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología.

---

11. Para más información sobre el Comité del Convenio sobre la Ciberdelincuencia (T-CY) véase: www.coe.int/en/web/cybercrime/tcy
12. Más información sobre la Oficina del Programa de Lucha contra la Ciberdelincuencia (C-PROC) está disponible en: www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-



CAPÍTULO 4.

INSTRUMENTOS INTERNACIONALES Y REGIONALES QUE ABARCAN LA CUESTIÓN DE LA VIOLENCIA CONTRA LAS MUJERES EN LÍNEA Y FACILITADA POR LA TECNOLOGÍA

Como se menciona en su preámbulo, el Convenio de Estambul se basa en instrumentos existentes y futuros que abarcan cuestiones relacionadas con la violencia de género contra las mujeres, incluidos la Convención sobre la Eliminación de todas las formas de discriminación contra la mujer (CEDAW), el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, la Carta Social Europea, el Convenio del Consejo de Europa sobre la Lucha contra la Trata de Seres Humanos y el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual.

Existen también otros instrumentos, acuerdos y políticas a nivel internacional y regional que tratan más específicamente de la cuestión de la violencia contra las mujeres en línea y facilitada por la tecnología (Simonovic, 2020).

Algunos instrumentos, textos y declaraciones recientes han ampliado la definición de violencia de género contra las mujeres o de sexismo para reconocer las formas específicas que se dan en línea y con el empleo de las nuevas tecnologías.

Recomendación General nº 35 del Comité de la CEDAW

La Recomendación General nº 35 adoptada por el Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW) respecto de la violencia de género contra las mujeres, que actualiza la Recomendación General nº 19 (Comité para la Eliminación de la Discriminación contra la Mujer 2017), define la violencia de género contra las mujeres como la que "se manifiesta en una serie de formas múltiples, interrelacionadas y recurrentes, en diversos ámbitos, del privado al público, incluidos entornos mediados por la tecnología, y trasciende las fronteras nacionales en el mundo globalizado contemporáneo", y añade que

> la violencia por razón de género contra la mujer se produce en todos los espacios y esferas de la interacción humana, ya sean públicos o privados, entre ellos los contextos de la familia, la comunidad, los

espacios públicos, el lugar de trabajo, el esparcimiento, la política, el deporte, los servicios de salud y los entornos educativos, y en la redefinición de lo público y lo privado a través de entornos tecnológicos , como las formas contemporáneas de violencia que se producen en línea y en otros entornos digitales.

El informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, en relación con la violencia contra las mujeres en línea define el fenómeno como

> Todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por éste, 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/HRC/38/47)

Recomendación del Consejo de Europa sobre la prevención y la lucha contra el sexismo

En marzo de 2019, el Comité de Ministros del Consejo de Europa adoptó una nueva recomendación sobre la prevención y la lucha contra el sexismo que contiene la primera definición de sexismo acordada internacionalmente, que incluye las nuevas tecnologías en línea y a través de ellas, y reafirma la existencia de un continuo de formas de violencia que afecta a las mujeres y las niñas (Consejo de Europa, 2019). A los efectos de esa Recomendación, se entiende por sexismo:

> Cualquier acto, gesto, representación visual, manifestación oral o escrita, práctica o comportamiento, basado en la idea de que una persona o grupo de personas es inferior por razón de su sexo, que tenga lugar en el ámbito público o privado, en línea o fuera de ella, cuyo propósito o efecto sea:
>
> i. Vulnerar la dignidad intrínseca o los derechos de una persona o grupo de personas; o
> ii. Provocar daño o sufrimiento físico, sexual, psicológico o socioeconómico a una persona o grupo de personas; o
> iii. crear un entorno intimidatorio, hostil, degradante, humillante u ofensivo; o
> iv. constituir un obstáculo a la autonomía y la plena realización de los derechos humanos de una persona o grupo de personas; o
> v. preservar y reforzar los estereotipos de género.

La recomendación añade que "los comportamientos sexistas, como, en particular, el discurso de odio sexista, pueden aumentar hasta desembocar o incitar la realización de acciones manifiestamente ofensivas y amenazantes, incluidos el abuso o violencia sexual, la violación o incluso acciones potencialmente letales. También pueden provocar la pérdida de recursos, las autolesiones o el suicidio", y subraya que "el sexismo y los comportamientos sexistas se producen en todos los aspectos de la actividad humana, incluido el ciberespacio (Internet y redes sociales). Una persona o grupo de personas puede experimentarlo individual o colectivamente, incluso si no son objeto directo de tales comportamientos". La recomendación también afirma que "Internet ha proporcionado un nuevo espacio para la expresión y transmisión del sexismo, especialmente el discurso de odio sexista, a un amplio público, a pesar de que el origen del sexismo no se encuentra en la tecnología, sino en las persistentes desigualdades de género." Por último, la recomendación reafirma la dimensión interseccional del sexismo y subraya circunstancias agravantes como las relaciones de poder y el alcance y la repetición del abuso. Esta definición de sexismo en el contexto de las comunicaciones digitales es única hasta la fecha.

Estrategia de Igualdad de Género del Consejo de Europa

La Estrategia de Igualdad de Género 2018-2023 del Consejo de Europa reafirma la existencia de formas de discriminación y violencia que afectan a los derechos, la seguridad y la protección de las mujeres tanto en línea como fuera de ella.

> Los contenidos digitales violentos y degradantes, también en la pornografía, así como la normalización de la violencia sexual, en especial, la violación, refuerzan la idea de la sumisión de las mujeres y fomentan que se las trate como miembros subordinados de la familia y de la sociedad. Se nutren de ellos la violencia

> contra la mujer, la incitación sexista al odio centrada en las mujeres, en especial, las feministas, y contribuyen a mantener y reforzar los estereotipos de género y el sexismo. (Consejo de Europa, 2018b)

De hecho, la Estrategia destaca la idea de un continuo de formas de violencia contra las mujeres, que se alimenta de estereotipos degradantes y comportamientos normalizados que se manifiestan tanto en línea como fuera de ella:

> también ha quedado demostrado que las redes sociales, en concreto, son objeto de uso abusivo y que, a menudo, mujeres y niñas sufren amenazas violentas y sexualizadas en la red. Las redes sociales y los videojuegos figuran entre las plataformas concretas que actúan como transmisores de la incitación sexista al odio. Con frecuencia, la libertad de expresión se desvirtúa como excusa para amparar conductas inaceptables y ofensivas. Al igual que sucede con otras formas de violencia contra la mujer, sigue sin denunciarse la incitación sexista al odio, pero sus efectos para la mujer, ya sean emocionales, psicológicos o físicos, pueden ser desoladores, en especial, para las chicas y mujeres jóvenes. Con el sexismo sucede lo mismo.

Varios elementos de la política de la UE también se centran en la cuestión de la violencia contra las mujeres en línea y facilitada por la tecnología, reconociendo el problema y elaborando hojas de ruta para luchar contra ella.

Estrategia de Igualdad de Género de la UE

La Estrategia de Igualdad de Género 2020-2025 de la UE reconoce la violencia contra las mujeres en línea y facilitada por la tecnología y al respecto señala que:

> La violencia en línea dirigida a las mujeres ha proliferado, con consecuencias concretas alarmantes. Esto es inaceptable. Supone un obstáculo a la participación de las mujeres en la vida pública. El acoso, la intimidación y los insultos en las redes sociales tienen repercusiones profundas en la vida cotidiana de las mujeres y las niñas. La Comisión propondrá la norma de servicios digitales para esclarecer las responsabilidades de las plataformas en línea con respecto a los contenidos difundidos por los usuarios. La norma de servicios digitales aclarará qué medidas se espera que apliquen las plataformas a la hora de atajar las actividades ilícitas en línea, al tiempo que protegen los derechos fundamentales. Los usuarios también tienen que ser capaces de actuar ante otros tipos de contenidos abusivos y nocivos, que no siempre se consideran ilícitos pero que pueden tener consecuencias devastadoras. Con objeto de proteger la seguridad en línea de las mujeres, la Comisión facilitará el desarrollo de un nuevo marco de cooperación entre las plataformas de internet. (Comisión Europea, 2020a).

En su respuesta a una pregunta parlamentaria del 13 de agosto de 2020, Helena Dalli, Comisaria de Igualdad, añadió que "de conformidad con la Estrategia Europea de Género, la Comisión facilitará el desarrollo de un marco de cooperación entre las plataformas y otras Partes interesadas para luchar contra la violencia de género en línea" (Parlamento Europeo, 2020).

Estrategia de la UE sobre los Derechos de las Víctimas

La Estrategia de la UE sobre los Derechos de las Víctimas define la ciberdelincuencia como "cualquier tipo de delito que se cometa en línea o con el uso de herramientas informáticas o en línea". Además, añade:

> La ciberdelincuencia puede consistir en delitos graves contra las personas, como los delitos sexuales en línea (incluidos los delitos contra los menores), la usurpación de identidad, los delitos de odio en línea. ... Las víctimas de ciberdelincuencia no siempre encuentran la asistencia adecuada para reparar los daños sufridos y, a menudo, no denuncian los delitos. ... Debe facilitarse aún más la denuncia de la ciberdelincuencia y debe proporcionarse a las víctimas la ayuda que necesitan. (Comisión Europea, 2020b)

Esa definición es interesante ya que plantea que la ciberdelincuencia es un problema que puede afectar a cualquier persona en línea, a través de cualquier medio.

Gran número de instrumentos entran en juego por lo que se refiere a la cuestión de la ciberdelincuencia en general y de la ciberdelincuencia contra las mujeres en particular, así como a cuestiones conexas que influyen

en los posibles remedios para la violencia contra las mujeres en línea y facilitada por la tecnología, tales como la protección de la intimidad, la responsabilidad de los intermediarios y la obtención de pruebas digitales. Algunos instrumentos y reglamentos de la UE, como el Reglamento General de Protección de Datos (RGPD), la Ley de Servicios Digitales (DSA), y el Reglamento sobre pruebas electrónicas son y seguirán siendo jurídicamente vinculantes para los Estados miembros. Otros instrumentos, que tratan de la cooperación con el sector privado, por ejemplo, como el Código de Conducta para la lucha contra la incitación ilegal al odio en Internet, se consideran instrumentos de autorregulación; con todo, en la práctica han sido eficaces hasta cierto punto para poner freno al fenómeno (el Código de Conducta mencionado ha sido útil para luchar contra la incitación ilegal al odio en las redes sociales).

El Convenio 108+ del Consejo de Europa y el RGPD

El objetivo del Convenio 108 original del Consejo de Europa sobre protección de datos es "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la intimidad, con respecto al tratamiento automatizado de los datos de carácter personal". Modernizado en 2018, y conocido ahora como el "Convenio 108+, Convenio para la protección de las personas con respecto al tratamiento de datos personales", garantiza que toda persona está cubierta por su protección, independientemente de su nacionalidad, siempre que se encuentre dentro de la jurisdicción de una de las Partes que han ratificado el Convenio (Consejo de Europa, 2018a). El ámbito de aplicación de la protección incluye tanto el tratamiento automatizado como el no automatizado de los datos personales y garantiza la protección de los datos sensibles, como los genéticos y biométricos, así como el "derecho de supresión".

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea (Reglamento (UE) 2016/679), que entró en vigor el 25 de mayo de 2018, regula la recogida y el tratamiento por parte de personas, empresas u organizaciones de los datos personales de los individuos en la UE. El Reglamento mejora los derechos de las personas respecto del control, la supresión, la rectificación, la restricción o la objeción al tratamiento de datos personales y facilita el acceso y la transferencia de sus datos personales, incluidos los datos de imagen como las imágenes íntimas no consentidas. El Reglamento también obliga a las empresas y entidades que procesan datos a solicitar el consentimiento explícito del usuario. "El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen".

El Reglamento se aplica si el responsable del tratamiento de los datos (una organización que recoge datos de residentes en la UE), el encargado del tratamiento (una organización que procesa datos en nombre de un responsable del tratamiento, como los proveedores de servicios en la nube) o el interesado (persona física) tiene su sede en la UE.

Como tal, ofrece posibilidades para frenar algunos aspectos de la violencia contra las mujeres en línea y facilitada por la tecnología; por ejemplo, exige que las empresas integren el respeto de la intimidad en el diseño de sus productos (sobre la cuestión del software de acoso, véase Citizen Lab, 2020). Asimismo, dispone que las personas responsables de subir material de abuso sexual basado en imágenes, así como los editores de dicho material, son considerados de manera conjunta controladores de datos y que, por lo tanto, estarán sujetos a las obligaciones y sanciones impuestas por el RGPD (Van der Wilk, 2018). Por otra parte, el RGPD incluye también el "derecho de borrado", más conocido como el derecho al olvido:

> Las disposiciones incluyen un nuevo derecho para los interesados que ya no desean que sus datos sean procesados, los que podrán solicitar su supresión definitiva, si no existen motivos legítimos para conservarlos ... Este derecho de supresión es de aplicación general, y no está restringido solo a los motores de búsqueda; por lo tanto, las nuevas disposiciones de la legislación de protección de datos de la UE proporcionan ahora a las víctimas de la pornografía de venganza no solo una forma de eliminar los enlaces a las imágenes difundidas, sino también un medio para eliminar las imágenes de los sitios web de origen, al menos dentro de la jurisdicción de la UE. (Setterfield, 2019)

La Ley de Servicios Digitales de la UE

La Directiva sobre el comercio electrónico, que entró en vigor el 8 de junio de 2000, estableció normas armonizadas para el comercio electrónico, incluidas las relativas a la responsabilidad de los proveedores de servicios, como las plataformas de comercio electrónico y las redessociales, por ejemplo. Incluye exenciones de

responsabilidad para determinados proveedores de servicios en línea teniendo en cuenta que desempeñan un papel neutral en relación con los contenidos transmitidos y/o alojados. Los proveedores de servicios tienen la obligación de eliminar o impedir el acceso a los contenidos ilegales alojados en sus plataformas tan pronto como reciban una notificación al respecto. Asimismo, el texto permite a los Estados miembros exigir a los proveedores de servicios la eliminación de los contenidos ilegales. Por lo tanto, la Ley proporciona una base jurídica para la denuncia y la retirada de contenidos ilegales en línea (Van der Wilk, 2018).

En 2019, se abrieron a revisión las principales disposiciones de la Directiva sobre el comercio electrónico y la Comisión Europea propuso la nueva Ley de Servicios Digitales con el fin de modernizar el marco jurídico de los servicios digitales.

La propuesta de la Ley de Servicios Digitales (DSA por sus siglas en inglés) se publicó en diciembre de 2020 y se espera que su adopción tome aproximadamente un año y medio. La propuesta establece "obligaciones claras de diligencia debida para determinados servicios intermediarios, como procedimientos de notificación y acción en relación con los contenidos ilícitos y la posibilidad de impugnar las decisiones de moderación de contenidos de las plataformas; la propuesta trata de mejorar la seguridad de los usuarios en línea en toda la Unión y reforzar la protección de sus derechos fundamentales" (Comisión Europea, 2020d).

La propuesta establece normas para las plataformas de muy gran tamaño, como los gigantes de las redes sociales, y aclara las "responsabilidades de los servicios digitales para abordar los riesgos a los que se enfrentan sus usuarios y proteger sus derechos". Mantiene el régimen de responsabilidad heredado de la Directiva sobre el comercio electrónico: las empresas que alojan contenidos no son responsables de los mismos a menos que tengan conocimiento de su aspecto ilegal. Si se presenta una objeción, la propuesta actual obliga a las empresas a retirar el contenido rápidamente. Por otra parte, la DSA incluye propuestas presentadas por grupos de derechos humanos para que en cada Estado miembro sea designado un "Coordinador de Servicios Digitales", que será la autoridad responsable de supervisar el cumplimiento de la normativa y de establecer mecanismos de reclamación y reparación y de resolución extrajudicial de litigios en los casos en que el contenido haya sido eliminado de manera injustificada.

> La propuesta solo exigirá la retirada de contenidos ilícitos e impondrá salvaguardias obligatorias cuando se retire información de los usuarios, que incluirán ofrecer explicaciones al usuario, unos mecanismos de reclamación facilitados por los prestadores de servicios y un mecanismo de resolución extrajudicial de litigios. Además, garantizará que los ciudadanos de la UE también estén protegidos cuando utilicen los servicios prestados por prestadores no establecidos en la Unión pero activos en el mercado interior, dado que esos prestadores también están cubiertos. (Comisión Europea, 2020d)

Por último, la propuesta menciona la obligación de que las mayores plataformas en línea permitan el acceso a los datos a investigadores acreditados, bajo la supervisión del Coordinador de Servicios Digitales.

La propuesta en materia de pruebas electrónicas

Según la Comisión Europea, "más de la mitad de todas las investigaciones penales actuales incluyen una solicitud transfronteriza de acceso a pruebas electrónicas como textos, correos electrónicos o aplicaciones de mensajería" (Comisión Europea, 2019).

En 2019, la Comisión Europea propuso iniciar negociaciones internas sobre el acceso transfronterizo a las pruebas electrónicas y emitió una "Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de presentación y conservación de pruebas electrónicas en materia penal" y la correspondiente "Directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas sobre la designación de representantes legales a efectos de la obtención de pruebas en los procesos penales". Ambas propuestas legislativas pretenden aportar más claridad jurídica y acelerar el proceso de obtención de pruebas electrónicas, "con la obligación de que los proveedores de servicios respondan en un plazo de diez días y hasta de seis horas en casos de urgencia (frente a una media de diez meses en el procedimiento de asistencia judicial mutua)". Este Reglamento permitiría a los organismos de aplicación de la ley de cualquier Estado miembro de la UE acceder más rápidamente a la información electrónica. Podrán pedirla directamente o solicitar su conservación a los proveedores de servicios en línea de otros países de la UE, en los casos en que la investigación de un delito esté contemplada en el Reglamento. La información o los datos electrónicos pueden ser textos, mensajes, correos electrónicos o información que permita la identificación del agresor, como su dirección IP. Asimismo, los instrumentos legislativos obligarían a los proveedores de servicios a "designar un representante legal en la Unión: para garantizar que todos los proveedores que

ofrecen servicios en la Unión estén sujetos a las mismas obligaciones, incluso si su sede se encuentra en un tercer país" (Comisión Europea, 2019).

El Reglamento propuesto permitirá atender los casos urgentes y acelerará los procesos para acceder a las pruebas en otros Estados miembros de la UE.

Al igual que el próximo Segundo Protocolo Adicional al Convenio de Budapest, el valor añadido de la Propuesta de Reglamento sobre las órdenes europeas de entrega y conservación de pruebas electrónicas consiste en tomar en cuenta el hecho de que hoy en día la mayoría de los delitos tienen una dimensión electrónica y que las pruebas y la información están almacenadas a veces fuera del país de residencia de la víctima.

La contraparte estadounidense de la Propuesta de Reglamento sobre las pruebas electrónicas, la *Clarifying Lawful Overseas Use of Data Act* (CLOUD Act), es una ley que permite a los países asociados de los Estados Unidos obtener directamente la cooperación de los proveedores de servicios de un país asociado. Hasta la fecha, sólo el Reino Unido reúne los requisitos de país asociado.

Además de los instrumentos citados, el futuro Plan de Acción Europeo para la Democracia y la *Estrategia* de la *UE para* una *Unión de la Seguridad* también contienen referencias a los contenidos perjudiciales y/o ilegales en línea.

Otro instrumento, adoptado hace ya algunos años, ha permitido alcanzar algunos resultados en la lucha contra la incitación ilegal al odio en línea.

El Código de conducta de la UE para la lucha contra la incitación ilegal al odio en Internet

En mayo de 2016, Facebook, Microsoft, Twitter y YouTube subscribieron el "Código de conducta para la lucha contra la incitación ilegal al odio en internet" de la Comisión Europea. Instagram, Snapchat y Dailymotion lo subscribieron en 2018, Jeuxvideo.com, en 2019 y TikTok, en septiembre de 2020.

Los signatarios del Código de conducta se han comprometido a examinar las denuncias de incitación al odio en sus plataformas y a responder a los contenidos ilícitos en un plazo de 24 horas. Las Partes definen la incitación ilegal al odio sobre la base de la "Decisión marco del Consejo relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia mediante el Derecho penal" (Unión Europea 2008). La definición abarca la incitación pública a la violencia o al odio dirigida contra un grupo de personas o un miembro de ese grupo, definido por referencia a la raza, el color, la religión, la ascendencia o el origen nacional o étnico. La quinta ronda de control del Código de conducta (2019-20) arroja que el 90 por ciento de las notificaciones se examinan en un plazo de 24 horas y que el 71 por ciento de los contenidos se eliminan. El motivo más común del discurso de odio en línea en 2020 fue la orientación sexual, que representó un 33 por ciento de las notificaciones. Esto se explica en parte por el hecho de que "las organizaciones que trabajan por los derechos LGBTQI han sido más activas a la hora de señalar contenidos" (Comisión Europea, 2020c).

Las principales deficiencias de esta actividad de vigilancia son la falta de un desglose de los datos y la falta de transparencia general acerca de las denuncias y las eliminaciones. No se tienen en cuenta los ataques interseccionales, lo que complica la plena comprensión del fenómeno del discurso de odio en línea, que contiene una fuerte dimensión interseccional y, por lo tanto, trivializa la experiencia de muchas usuarias.[13] Asimismo, en el estudio del Consejo de Europa "Modelos de Gobernanza del Discurso de Odio en Línea", Alexander Brown ha señalado que este ejercicio de vigilancia presenta dos problemas principales:

> A las plataformas de Internet se les comunica las fechas del período de control. Debido a ello, no está claro si las variaciones de los porcentajes representan auténticas mejoras de la tasa de eliminación de la incitación ilegal al odio durante todo el año o si, por el contrario, reflejan una mayor capacidad de las plataformas de Internet para manipular el proceso de control, mejorando de modo apreciable las tasas de eliminación solamente durante el período en que se lleva a cabo la supervisión. (Consejo de Europa, 2020a).

Por otra parte, el autor señala que las plataformas de Internet ofrecen "subvenciones publicitarias" a organizaciones activas que participan en las sesiones y reuniones de formación en materia de vigilancia (permitiéndoles,

13. Amnistía Internacional informa, por ejemplo, que las mujeres políticas y periodistas negras corren un 84 por ciento más de riesgo de recibir comentarios abusivos en Twitter que las mujeres blancas. Allen, K., Amnistía Internacional Reino Unido (2020), "UK: Online Abuse against Black Women MPs 'Chilling'", disponible en: www.amnesty.org.uk/press-releases/uk-online-abuse-against-black-women-mps-chilling.

por ejemplo, organizar campañas gratuitas en las plataformas); ello plantea dudas al respecto sobre la independencia, neutralidad y transparencia de esas organizaciones.

La dimensión digital de la violencia se toma cada vez más en cuenta en todo el mundo. La "Observación General 25 del Comité de los Derechos del Niño de la ONU sobre los derechos del niño en relación con el entorno digital" es un ejemplo reciente de la manera en que los tratados de derechos humanos están respondiendo a un nuevo entorno de amenazas.[14] A nivel de la UE, en la actualidad se da prioridad a la ratificación del Convenio de Estambul, pero la Presidenta Von der Leyen también ha anunciado varias iniciativas clave para 2021 que podrían responder a las formas de violencia contra las mujeres en línea y facilitada por la tecnología. En estos momentos se está estudiando una propuesta legislativa para prevenir y combatir formas específicas de violencia de género, así como propuestas para ampliar la lista de delitos de la UE a todas las formas de delitos de odio y de incitación al odio.[15] Algunos grupos de defensa de los derechos de las mujeres también han abogado por un marco jurídico integral y una directiva sobre la prevención y la lucha contra la violencia contra las mujeres que permita una concertación entre los instrumentos existentes, reconozca la violencia en línea y defina explícitamente los tipos de violencia contra las mujeres en línea y facilitada por la tecnología.[16]

A continuación exploraremos hasta qué punto los dos tratados del Consejo de Europa, el Convenio de Estambul y el Convenio de Budapest, pueden contribuir a abordar la violencia contra las mujeres en línea y facilitada por la tecnología mediante las políticas, la prevención, la protección, el enjuiciamiento y la cooperación internacional.

De hecho, a nivel del Consejo de Europa, las sinergias entre los tratados ofrecen la posibilidad de desarrollar respuestas coordinadas a este fenómeno. En la siguiente parte exploraremos más a fondo esa complementariedad; para ello, se definirán las formas de violencia en línea, se las relacionará con las disposiciones del Convenio de Estambul, y en la medida de lo posible, se las complementará con las disposiciones sustantivas del Convenio de Budapest. Se explorarán tres amplias categorías de violencia en línea, con arreglo al artículo 40 (acoso sexual), al artículo 34 (acoso) y al artículo 33 (violencia psicológica) del Convenio de Estambul: 1) acoso sexual y de género en línea; 2) acoso en línea y facilitado por la tecnología, y 3) formas de violencia psicológica en línea y facilitada por la tecnología, incluida la incitación al odio sexista.

14. Convención de las Naciones Unidas sobre los Derechos del Niño (2021), Comité de los Derechos del Niño, "Observación general nº 25 (2021) sobre los derechos del niño en relación con el entorno digital", disponible en: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFO6kx0VqQk6dNAzTPSRNx0n7GJ58W3UK1vGY9AULNbeXIno%2f66dzxFq8S5kEpb2Uv .
15. Von der Leyen U. y Šefčovič M., Comisión Europea (2020), Estado de la Unión 2020, "Carta de intención al Presidente David Maria Sassoli y a la Canciller Angela Merkel", disponible en: https://ec.europa.eu/info/sites/info/files/state_of_the_union_2020_letter_of_intent_en.pdf.
16. Entrevista con Asha Allen, European Women's Lobby, septiembre de 2020, https://womenlobby.org/?lang=en.

CAPÍTULO 5.
EXAMEN DE LOS ARTÍCULOS 33, 34 Y 40 DEL CONVENIO DE ESTAMBUL

En este capítulo se presentará una categorización de los tipos de violencia contra las mujeres en línea y facilitada por la tecnología, sobre la base de investigaciones recientes en este campo. Existen varios tipos de categorización que son igualmente válidos para comprender el fenómeno.[17] En algunos casos, las formas de violencia contra las mujeres en línea y facilitada por la tecnología se han clasificado y planteado atendiendo a la relación entre la víctima y el agresor; en otros, la clasificación ha estado basada en las modalidades de la conducta de abuso, o en los medios empleados para perpetrar los actos de violencia sexual. Algunas clasificaciones jurídicas se centran en la dimensión informática del abuso, no toman en cuenta la dimensión de género ni contemplan esos tipos de violencia en el marco de las violaciones de derechos como el derecho a la intimidad o los derechos de propiedad intelectual. A continuación se propone una categorización que define cada tipo de violencia con arreglo al marco del Convenio de Estambul y a las disposiciones aplicables del Convenio de Budapest.

De hecho, los artículos 33, 34 y 40 del Convenio de Estambul abarcan gran número de formas de violencia perpetradas en línea y facilitadas por el uso de nuevas tecnologías. A continuación se define cada una de las categorías, se indica el vínculo a la definición del Convenio de Estambul y se añaden otras definiciones cuando están disponibles. Además, se presenta una definición exhaustiva de cada forma de violencia, seguida de ejemplos, y se examinan los artículos aplicables del Convenio de Budapest.

Acoso sexual y de género en línea

Nota sobre el ciberacoso escolar [*cyberbullying*]

Por ciberacoso escolar se entiende una forma de acoso cibernético que suele afectar a los menores, independientemente de su género. Consiste en un comportamiento agresivo en línea de manera reiterada que persigue atemorizar y socavar la autoestima o la reputación de alguien y puede provocar depresión en personas vulnerables o incluso llevarlas a considerar el suicidio.

El Convenio de Estambul define el acoso sexual en su artículo 40 como "toda forma de comportamiento no deseado, verbal, no verbal o físico, de carácter sexual, que tenga por objeto o resultado violar la dignidad de una persona, en particular cuando dicho comportamiento cree un ambiente intimidatorio, hostil, degradante,

17. Véase, por ejemplo, Consejo de Europa 2018c; Harris 2020b; Hinson et al., 2018.

humillante u ofensivo". El Convenio establece que el acoso sexual debe ser objeto de sanciones penales u otras sanciones legales. Además, el Convenio contempla en el artículo 46 circunstancias agravantes cuando "el delito se haya cometido contra un cónyuge o pareja de hecho actual o antiguo, de conformidad con el derecho interno, por un miembro de la familia, una persona que conviva con la víctima o una persona que abuse de su autoridad" (46a); "el delito, o los delitos conexos, se haya cometido de forma reiterada (46b); "el delito se haya cometido contra una persona que se encuentre en situación de vulnerabilidad por la concurrencia de particulares circunstancias" (46c); " el delito se haya cometido por dos o más personas actuando conjuntamente" (46e) y "el delito haya provocado graves daños físicos o psicológicos a la víctima" (46h).

En cuanto a otras definiciones, la encuesta más reciente sobre la violencia contra las mujeres llevada a cabo por la Agencia de la Unión Europea para los Derechos Fundamentales (2014) define el acoso sexual en línea como "correos electrónicos o mensajes SMS sexualmente explícitos no deseados que ofenden, insinuaciones inapropiadas que ofenden en sitios web de redes sociales como Facebook, o en salas de chat de Internet". Los resultados de la encuesta muestran que en 2014, el 20 por ciento de las mujeres jóvenes de la Unión Europea habían sufrido ciberacoso sexual. El proyecto de investigación DeShame (centrado en los menores), financiado por la UE, propone una definición exhaustiva del acoso sexual en línea: "conducta sexual no deseada que tiene lugar en cualquier plataforma digital" (Childnet/Save the Children/UCLan 2019). Se reconoce como una forma de violencia sexual y abarca una "amplia gama de comportamientos que utilizan contenidos digitales (imágenes, vídeos, publicaciones, mensajes, páginas) en diversas plataformas (privadas o públicas) que pueden hacer que una persona se sienta amenazada, explotada, coaccionada, humillada, molesta, sexualizada o discriminada". En sí misma, esa definición retoma la del Convenio de Estambul, pero añade los ámbitos en que puede darse ese tipo de conducta. El grupo de investigadores que participa en el proyecto ha presentado una interesante categorización del acoso sexual en línea: 1) difusión no consentida de imágenes o vídeos; 2) explotación, coacción y amenazas; 3) ciberacoso escolar sexualizado. Esas tres categorías engloban la gran mayoría de los casos de violencia en línea de que son víctimas las mujeres. A continuación se adoptará esa categorización para agrupar las diferentes formas de acoso sexual y de género en línea.

Difusión no consentida de imágenes o vídeos

La difusión no consentida de imágenes o vídeos o la difusión no consentida de material explícito, que puede manifestarse de muchas formas diferentes, es una forma generalizada y cada día más frecuente de violencia en línea y facilitada por las nuevas tecnologías.

En un estudio internacional sobre las víctimas y los autores de abuso sexual basado en imágenes, el conjunto de delitos se define como "la toma de imágenes (fotos o vídeos) de desnudos o de carácter sexual de una persona, su difusión no consentida o las amenazas de diseminarlas. Esto también incluye imágenes alteradas digitalmente en las que el rostro o el cuerpo de una persona se superpone o se "cose" en una foto o un vídeo pornográfico, lo que se conoce como "pornografía falsa" (incluidos los "ultrafalsos", imágenes sintéticas creadas utilizando inteligencia artificial)". Los autores señalan que "una de cada tres encuestadas informó que alguien les había tomado una imagen desnuda o de carácter sexual sin su consentimiento; una de cada cinco informó que alguien había distribuido una imagen suya desnuda o de carácter sexual sin su consentimiento (20,9 por ciento), y casi una de cada cinco informó que alguien la había amenazado con difundir una imagen desnuda o de carácter sexual de ellas (18,7 por ciento)". El estudio también llegó a la conclusión de que esa forma de violencia "abarca muy diversos contextos relacionales y perjuicios, así como una multitud de efectos diferenciales para las víctimas. El estudio reveló que las mujeres experimentan el abuso sexual basado en imágenes de distintas maneras en el contexto de múltiples experiencias de daños interpersonales y de victimización, incluidos el acoso físico, la violencia sexual y/o las situaciones de abuso por parte de la pareja" (Powell et al., 2020).

Imágenes/vídeos sexuales tomados sin consentimiento y difundidos en línea o voyeurismo digital

Esta forma de comportamiento violento incluye las "imágenes rastreras" [*creepshots*] (fotos sexuales o íntimas tomadas en entornos públicos o privados sin consentimiento ni conocimiento de la víctima y difundidas en línea) y las fotos debajo de las faldas [*upskirting*] (fotos sexuales o íntimas tomadas debajo de la falda o el vestido de la víctima, sin su consentimiento y difundidas en línea). En relación con las fotos debajo de las faldas se suele mencionar el caso de Gina Martin, joven británica que asistía a un festival y que fue fotografiada debajo de su falda mientras hacía cola para ir al baño. Más tarde elevó su caso al Parlamento. En la actualidad, el tomar fotos debajo de las faldas se considera un delito en el Reino Unido; los culpables se enfrentan a hasta dos años de cárcel.[18]

18. Ministerio de Justicia del Reino Unido (2019), "Upskirting: Know Your Rights", disponible en: www.gov.uk/government/news/upskirting-know-your-rights.

Imágenes/vídeos sexuales tomados de forma consentida pero difundidas sin consentimiento[19]

La difusión de imágenes y vídeos sexuales de las víctimas sin su consentimiento constituye abuso sexual basado en imágenes (McGlynn, Rackley y Houghton, 2017). El abuso sexual basado en imágenes se ha denominado también "explotación sexual basada en imágenes" (Powell y Henry, 2016); "intercambio de imágenes o vídeos no consentidos", o "imágenes íntimas no consentidas"[20] (NCII por su sigla en inglés); pornografía no consentida (Citron y Franks, 2014), o "pornografía vengativa" o "pornografía de venganza". De hecho, en muchos estudios se hace hincapié en la necesidad de redefinir el término "pornografía de venganza" utilizado en los medios de comunicación, ya que describe la experiencia del agresor en lugar del maltrato incesante de que es objeto la víctima.

El agresor (ex pareja o pareja actual, amigo, pariente, conocido o desconocido) obtiene imágenes o vídeos en el transcurso de una relación, o las piratea o roba del ordenador, las cuentas de redes sociales o el teléfono de la víctima. Más tarde, el agresor difunde en línea las fotografías/vídeos, lo que da lugar a su difusión posterior por muchos agresores secundarios, que a veces se cuentan por millares. Las imágenes a veces van acompañadas de la dirección y los datos de contacto de la víctima, así como los de su familia o empleador; este fenómeno se ha denominado "doxeo" [*doxing*].

Ultrafalsos

Los "ultrafalsos" [*deepfakes*] son el resultado de un proceso que utiliza algoritmos y aprendizaje profundo para transformar digitalmente un rostro en un vídeo, y para manipular el sonido, con el fin de crear la ilusión de que se trata de otra persona (Langlais-Fontaine, 2020). Los "ultrafalsos" no están comprendidos en las categorías propuestas por el proyecto DeShame; con todo, en su estudio transnacional sobre el abuso sexual basado en imágenes Powell et al. (2020) han clasificado los "ultrafalsos" en la categoría de acoso sexual en línea.

Según un informe elaborado por la empresa holandesa Sensity (Ajder et al., 2019), el 96 por ciento de los vídeos ultrafalsos analizados eran vídeos pornográficos:

> La pornografía ultrafalsa es un fenómeno dirigido exclusivamente contra las mujeres, que se ven perjudicadas. En cambio, la mayoría de los vídeos ultrafalsos no pornográficos analizados en YouTube tenían sujetos masculinos. ... El ecosistema de la pornografía ultrafalsa se sustenta casi por completo en sitios web dedicados a la pornografía ultrafalsa, que albergaban 13.254 del total de vídeos [que] descubrieron; por el contrario, los sitios web de pornografía convencional sólo albergaban 802 vídeos.

La mayoría de las mujeres víctimas de ataques son personas famosas, principalmente actrices y cantantes, que representan el 81 por ciento de las víctimas. El resto de las víctimas de pornografía ultrafalsa son víctimas de lo que la investigadora Claire Langlais-Fontaine ha denominado abuso sexual basado en imágenes en el contexto de relaciones (anteriores) (Langlais-Fontaine, 2020).

Exhibicionismo cibernético

El exhibicionismo cibernético [*cyber flashing*] consiste en el envío de fotos sexuales no solicitadas e impuestas utilizando aplicaciones de citas, aplicaciones de mensajería o textos. También se emplea Bluetooth y Airdrop (combinación de Bluetooth y Wi-Fi, que crea un canal bidireccional entre teléfonos que se encuentran a menos de 10 metros de distancia). Este tipo de exhibicionismo prolifera en las redes sociales, las aplicaciones de mensajería y las aplicaciones de citas; también puede manifestarse en el transporte público, por ejemplo, cuando se recurre a Airdrop/Bluetooth. Esta forma específica de acoso sexual, tanto por parte de desconocidos como de personas conocidas, puede ser clasificada como acoso en el ámbito de la violencia doméstica; acoso sexual en la calle; exhibicionismo y acoso sexual por parte de desconocidos o compañeros (BBC 2019a).

Acoso sexual en línea con explotación, coacción y amenazas

La segunda categoría, correspondiente al acoso sexual en línea de mujeres y niñas, incluye explotación, coacción y amenazas. Esta segunda categoría de acoso sexual en línea abarca las diferentes formas de violencia que se enumeran a continuación.

19. El abuso sexual basado en imágenes se examina en el primer análisis sobre términos específicos (véase el Anexo 1).
20. Clasificado como tal por Facebook (s.f.).

Sexteo forzado

El sexteo [sexting] forzado consiste en acosar o presionar a una víctima en línea para que comparta imágenes sexuales de sí misma o participe en un comportamiento sexual en línea (o fuera de ella).

Investigaciones recientes demuestran que

> Las jóvenes consienten el sexteo debido a la presión ejercida por sus parejas o posibles parejas (Döring, 2012; Lippman y Campbell, 2014). En el contexto de las relaciones amorosas, suelen producirse situaciones en las que uno de los miembros de la pareja exige a la persona con la que mantiene relaciones íntimas que envíe contenido sexualmente explícitos, o incluso que participe en intercambios mutuos de ese tipo de contenidos (Döring, 2012; Lippman y Campbell, 2014).
>
> Algunas chicas dan su consentimiento al sexteo "no deseado", porque creen que es un tipo de "acuerdo sexual" o el "precio indeseable" que deben pagar para mantener una buena relación (Drouin y Tobin, 2014; Lippman y Campbell, 2014; Renfrow y Rollo, 2014). Por lo general, las chicas experimentan mayor presión para consentir al sexteo que los varones (Lippman y Campbell, 2014; Ringrose et al., 2012; Walker et al., 2013; Walgrave et al., 2013). (Dodaj y Sesar, 2020).

El sexteo forzado puede convertirse en sexteo violento en el contexto de la violencia doméstica, y también llegar a constituir abuso sexual basado en imágenes o sextorsión.

Sextorsión

La sextorsión, o/y el chantaje por webcam, es una forma de violencia en línea cada día más frecuente que consiste en amenazar con la publicación de contenidos sexuales (imágenes, vídeos, ultrafalsos, rumores sexuales) para amenazar, coaccionar o chantajear a una persona, ya sea para obtener contenido sexual adicional, o a cambio de dinero, y a veces por ambas cosas.

Roberta Liggett O'Malley y Karen M. Holt clasifican los diferentes tipos de sextorsión en cuatro categorías: la sextorsión cibernética centrada en menores; la sextorsión cibernética que constituye delito cibernético; la sextorsión cibernética íntima con violencia, y la sextorsión cibernética delictiva transnacional (Liggett O'Malley 2020). Cuando los niños y las niñas se ven afectados, Europol recomienda emplear el término "coerción sexual y extorsión de niños y niñas en línea", ya que el término sextorsión "no refleja que el acto en cuestión implica el abuso y la explotación sexual de un niño, con consecuencias sumamente graves para la víctima".

En Francia, por ejemplo, este delito está penado desde 2014 (2018) por el artículo 11 de la Ley sobre la violencia sexual y sexista (*Loi no. 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes*) que sanciona el acoso sexual en línea, y por el artículo 312-1 relativo a la extorsión. En Suiza, por el contrario, no está tipificado como delito; los delitos de extorsión sexual pueden ser enjuiciados en virtud del artículo 156 del Código Penal (extorsión y chantaje), del artículo 174 del Código Penal (calumnia), del artículo 179 (quáter) del Código Penal (violación de la intimidad) o del artículo 197 del Código Penal (pornografía)[21], sin que se tenga en cuenta necesariamente el aspecto de género del delito.

En el marco del Convenio de Estambul, la sextorsión de que son objeto las mujeres y las niñas puede clasificarse como una forma de acoso sexual en línea, con arreglo a su definición: "toda forma de comportamiento no deseado, verbal, no verbal o físico, de carácter sexual, que tenga por objeto o resultado violar la dignidad de una persona, en particular cuando dicho comportamiento cree un ambiente intimidatorio, hostil, degradante, humillante u ofensivo"; entre las posibles circunstancias agravantes se destaca "que el delito se haya cometido contra un cónyuge o pareja de hecho actual o antiguo, de conformidad con el derecho interno, por un miembro de la familia, una persona que conviva con la víctima o una persona que abuse de su autoridad" o/y "que el delito haya provocado graves daños físicos o psicológicos a la víctima".

Amenazas de violación

Las amenazas en línea de violencia sexual, como las amenazas de violación dirigidas a la víctima o a sus parientes, incluidos sus hijos, hijas, miembros de su familia, amigos, etc., son una de las formas más comunes de violencia que experimentan las mujeres en línea. Según el informe *Toxic Twitter* publicado por Amnistía Internacional, "las amenazas de violencia en línea contra las mujeres suelen estar sexualizadas e incluyen

21. Código Penal Suizo, disponible en: www.admin.ch/opc/fr/classified-compilation/19370083/index.html#a156.

referencias específicas al cuerpo de las mujeres. El objetivo de la violencia y del abuso es crear un entorno en línea hostil para las mujeres con el fin de avergonzarlas, intimidarlas, degradarlas, menospreciarlas o silenciarlas" (Amnistía Internacional, 2018). En el informe, Amnistía señaló que el 25 por ciento de las encuestadas, todas activas en Twitter, habían recibido amenazas dirigidas contra ellas y su familia, que incluían violencia sexual, dolor físico, incitación al suicidio y muerte. Esas amenazas suelen ir acompañadas de otras formas de expresión del odio basadas en la identidad percibida de la víctima.

Doxeo sexualizado/de género

Al igual que en otras formas de doxeo, la información personal se divulga en línea sin consentimiento para fomentar el acoso sexual. En Francia, el abuso sexual basado en imágenes relacionado con el doxeo se ha multiplicado durante los períodos de cuarentena de la Covid-19, habiendo aparecido nuevos tipos de cuentas de Snapchat o Telegram para ridiculizar en público denominadas "*ficha*" (término derivado del verbo francés "afficher", con el sentido de "ridiculizar en público") (Khouiel/Vice, 2020). Esas cuentas locales reenvían desnudos de mujeres jóvenes, algunas menores de edad, revelando su identidad y su información de contacto, dirigiendo contra ellas a pandillas que cometen abusos sexuales en su entorno local. Las cuentas "*fichas*" están tipificadas como difusión no consentida de imágenes, y los culpables pueden enfrentar hasta dos años de cárcel y una multa de 60.000 euros.

Ciberacoso acoso sexualizado

La tercera subcategoría de acoso sexual en línea incluye comportamientos como la difusión de chismes o rumores sobre el presunto comportamiento sexual de la víctima; la publicación de comentarios sexualizados al pie de las publicaciones o las fotos de la víctima; el hacerse pasar por la víctima; la difusión de contenido sexual o el acoso sexual de otras personas, con el consiguiente daño a su reputación y/o su modo de vida; el "sacar del armario" [*outing*] a alguien sin su consentimiento, o el "revelar el nombre anterior" [*deadnaming*] de una persona trans, empleando su nombre de nacimiento, con el propósito de asustar, intimidar o causar desvalorización del cuerpo [*bodyshaming*].

Como se ha visto, el acoso sexual en línea adopta muchas formas que, en algunos casos se solapan con el discurso de odio sexista y de género y con otros tipos de discurso de odio y acoso como los basados en la orientación sexual y las identidades de género. Esos diferentes tipos de violencia no son todos posibles infracciones penales per se. Con todo, la mayoría de ellos están normalizados y las víctimas deben valerse por sí mismas.

Disposiciones aplicables del Convenio de Budapest

Los artículos del Convenio de Estambul sobre el acoso sexual y las circunstancias agravantes enumerados anteriormente pueden enriquecerse y aclararse con una serie de disposiciones del Convenio de Budapest. A continuación se presenta una lista no exhaustiva, que sirve de ejemplo de las disposiciones sustantivas del Convenio de Budapest, y se destacan los aspectos fundamentales que guardan relación con el acoso sexual en línea.

Artículo 2 del Convenio de Budapest (Acceso ilícito)

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Esta disposición describe el acceso ilícito al sistema de una víctima, elemento común de las ciberamenazas, el ciberacoso, la sextorsión y otras formas de violación de la intimidad consideradas ciberviolencia. Se puede acceder de manera ilícita al sistema de un tercero con el fin de utilizarlo como plataforma para enviar mensajes, hacer ataques o robar datos íntimos.

Artículo 3 del Convenio de Budapest (Interceptación ilícita)

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema

> informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Esta disposición describe la interceptación de datos sin derecho.[22] Está relacionada relaciona con la escucha, el seguimiento o la vigilancia del contenido de las comunicaciones con el fin de obtener o grabar los datos personales (no públicos) de una víctima, empleando medios técnicos. El tráfico entrante o saliente puede ser interceptado de manera ilegal para dificultar la comunicación con las fuerzas del orden o para mostrar a la víctima que el atacante está al tanto de todo lo que hace la víctima. El tráfico también puede ser interceptado para cometer violaciones de la intimidad, como ocurre en los casos de y abuso sexual y de acoso basado en imágenes.

Artículo 8 del Convenio de Budapest (Fraude informático)

> Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; y b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Algunas formas de sextorsión pueden interpretarse como fraude informático, ya que los agresores pueden extorsionar imágenes íntimas o amenazar con hacerlo para exigir dinero a sus víctimas, a veces utilizando estrategias de piratería informática (CBC, 2017).

Artículo 10 del Convenio de Budapest (Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines)

> 1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual,... a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

El Informe explicativo del Convenio examina en mayor detalle los casos en que debe penalizarse las infracciones de la propiedad intelectual: "Cada Parte tiene la obligación de tipificar como delito las infracciones deliberadas de la propiedad intelectual y otros derechos conexos, a veces denominados derechos afines, derivados de los acuerdos enumerados en el Artículo, "cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático".

En los países en que no existe una ley sobre el abuso sexual basado en imágenes, las leyes de derechos de propiedad intelectual pueden ser la mejor herramienta disponible para las víctimas (O'Connell y Bakina, 2020).

Acoso en línea y facilitado por la tecnología

El Convenio de Estambul define el acoso en su artículo 34 como "el hecho, cuando se cometa intencionadamente, de adoptar, en varias ocasiones, un comportamiento amenazador contra otra persona que lleve a ésta a temer por su seguridad". El Convenio pide a las Partes que tipifiquen como delito ese comportamiento. El Informe explicativo del Convenio define con más detalle el acoso y la utilización de las TIC para perpetrar ese tipo de abuso:

> El comportamiento amenazante puede consistir en seguir repetidamente a otra persona, entablar una comunicación no deseada con otra persona, o hacerle saber que está siendo observada. Esto incluye perseguir físicamente a la víctima; presentarse en su lugar de trabajo, instalaciones deportivas o educativas, así como seguir a la víctima en el mundo virtual (salas de chat, sitios de redes sociales, etc.).

22. "Sin derecho" se define de la siguiente manera en el Informe explicativo del Convenio de Budapest "Conducta realizada sin autoridad (ya sea legislativa, ejecutiva, administrativa, judicial, contractual o consensual) o conducta que no está cubierta por defensas legales establecidas, excusas, justificaciones o principios relevantes en el derecho interno". Véase Consejo de Europa (2001b).

> La comunicación no deseada implica la búsqueda de cualquier contacto activo con la víctima a través de cualquier medio de comunicación disponible, incluidas las modernas herramientas de comunicación y las TIC. (Consejo de Europa, 2011b).

Las amenazas en línea (sexuales, económicas, físicas o psicológicas), el intento de empañar la reputación de la víctima; el monitoreo de las actividades en línea de la víctima para recoger información íntima; el robo de identidad; la solicitud de actos sexuales haciéndose pasar por la víctima, y la realización de una campaña de acoso colectivo para aislar a la víctima son ejemplos de prácticas de acoso que tienen lugar en la esfera digital. Para llevar a cabo tales violaciones de la intimidad los agresores suelen vigilar o espiar a la víctima en diversas plataformas de Internet o recurrir al empleo de herramientas digitales. En un estudio alemán a gran escala sobre el ciberacoso, los autores descubrieron que la mayoría de las víctimas eran mujeres, que la mayoría de los agresores eran hombres, y que el ciberacoso se producía principalmente en el contexto de la violencia doméstica (Dreßing et al., 2014). La última encuesta de la FRA sobre la violencia contra las mujeres reveló que el 14 por ciento de las mujeres de la UE han sido objeto de acoso, habiendo recibido comunicaciones ofensivas o amenazantes desde la edad de 15 años (acoso por medio de correo electrónico, mensajes de texto o Internet). Las principales víctimas son las mujeres jóvenes: El 4 por ciento de todas las mujeres de la UE entre los 18 y 29 años habían sido víctimas de ciberacoso durante los 12 meses anteriores a la entrevista, frente al 0,3 por ciento de las mujeres mayores de 60 años (FRA, 2014). Esas cifras se actualizarán una vez concluido el próximo estudio de la FRA sobre la violencia contra las mujeres que se realizará entre 2020 y 2022.

Por otra parte, un reciente informe encargado por Women's Aid muestra que el 45 por ciento de las víctimas de la violencia doméstica informaron haber sufrido algún tipo de abuso en línea durante su relación y el 48 por ciento informó haber sufrido acoso o abuso en línea por parte de su ex pareja una vez que la relación tocó a su fin. Un 38 por ciento declaró haber sufrido acoso en línea una vez que había concluido la relación, y el 75 por ciento manifestó su preocupación por el hecho de que la policía no haya sabido cómo responder mejor a los abusos o al acoso en línea. Esa cifra incluye al 12 por ciento que había presentado denuncias a la policía y no había recibido ayuda (Laxton/Women's Aid, 2014).

El objetivo general del acoso en línea y facilitado por la tecnología es atemorizar a la víctima y generar en ella un sentimiento de impotencia. Es una cuestión de poder y de control:

> Las supervivientes han descrito que sus parejas actuales o anteriores han activado los servicios de localización en sus dispositivos, y que sus hijos e hijas se han visto obligados a activar las funciones de vídeo durante las llamadas telefónicas con sus padres. En sí mismos, son actos que pueden parecer anodinos. Sin embargo, en realidad estaban encaminados a ejercer control: para acosar y localizar a una mujer, o conocer la dirección del centro de acogida o de su nueva residencia. Por lo tanto, Woodlock y yo proponemos que se utilice el término de control coercitivo en el marco digital para aludir al "uso de dispositivos y medios digitales para acosar, amenazar y maltratar a las parejas o ex parejas y a los hijos e hijas". (Salter et al., 2018)

En su estudio sobre lo que denomina violencia familiar y doméstica facilitada por la tecnología (VFDT), la Dra. Bridget Harris describe a los agresores que utilizan "dispositivos físicos... cuentas virtuales o electrónicas..., y software o plataformas..." para maltratar y coaccionar a las víctimas, que pueden ser "parejas íntimas actuales o anteriores, sus hijos, hijas, parejas sentimentales posteriores, amigos y familiares" (Harris, 2020a). La autora señala que "la VFDT es un término general que abarca una serie de comportamientos, incluido el uso de la tecnología para llevar a cabo otras formas de abuso (como el abuso sexual y el abuso financiero) y para facilitar el acoso tradicional (en persona)".

Algunos agresores recurren a la vigilancia o al espionaje en las redes sociales o de mensajería, creando cuentas falsas y "haciéndose amigos" o siguiendo a su víctima anónimamente, o incluso solicitando acceso a contraseñas. En un estudio estadístico sobre el acoso mediante el empleo de las nuevas tecnologías en el contexto de la violencia doméstica, los investigadores descubrieron que el agresor les había exigido sus contraseñas al 17 por ciento de las víctimas (Woodlock, 2017). Otros recurren a soluciones más refinadas de "alta tecnología" para amedrentar, amenazar y maltratar a sus víctimas, lo que se aborda en la siguiente sección. Con todo, las soluciones de bajo nivel tecnológico, como el acoso en las redes sociales o en las aplicaciones de mensajería, no son necesariamente menos dañinas que las que emplean tecnología avanzada:

> Se ha puesto de manifiesto que el contacto y el acoso abusivo y obsesivo con el empleo de la tecnología es una tendencia cada vez más frecuente en los casos de homicidio y filicidio relacionados con la violencia doméstica y familiar ... En un estudio reciente del Equipo de Evaluación de los Decesos del estado de

> Nueva Gales del Sur (2017, 134) se puso de manifiesto que los maltratadores acechaban a las víctimas en el 39 por ciento de los casos, antes de la agresión final, y que en más del 50 por ciento de los casos el agresor había recurrido a medios tecnológicos para acosar a la víctima de violencia doméstica, por ejemplo, enviando constantemente mensajes de texto, revisando el teléfono de la víctima, e interactuando con la víctima en las redessociales o en sitios de citas recurriendo a una identidad falsa. (ibíd.)

Por otra parte, algunas características de las redes sociales que podrían parecer inofensivas en situaciones no coercitivas son utilizadas para perpetrar ataques:

> Las plataformas suelen suponer que los posibles contactos son amistosos, si no neutrales, y que la ampliación del número de contactos es algo positivo. Facebook, con su lista de "personas que quizás conozcas", Twitter con sugerencias de "a quién seguir" e Instagram con su lista de "sugerencias para ti", animan a los usuarios a hacer amigos o a seguir a otros, sobre la base de asociaciones mutuas. Esto puede ser una función útil de las redes sociales; sin embargo, tiene implicaciones y podría representar una provocación para mujeres que han estado expuestas a la violencia por personas en círculos sociales más amplios. Bivens (2015) ha documentado cómo esas herramientas han puesto en contacto, inadvertidamente, a supervivientes de violencia sexual con los agresores, y la angustia resultante que experimentan las mujeres. De manera similar, las supervivientes de violencia doméstica han descrito factores desencadenantes cuando han sido invitadas a conectarse con miembros de la red social del agresor que han apoyado al agresor o participado con él para perjudicarlas (Harris y Woodlock, de próxima publicación). No cabe duda de que la tecnología puede ayudar a crear redes de agresores. DeKeseredy y Schwartz, 1993; y DeKeseredy, 1990 explican que, en las sociedades patriarcales, quienes ejercen la violencia pueden tener aliados de ideas afines que desarrollan, comparten y refuerzan los valores e ideologías que apoyan, justifican y normalizan la violencia. En el pasado, esas redes de apoyo de pares estaban conectadas en el mundo real, pero ahora están fomentadas por la tecnología. (ibíd.)

A continuación se define un pequeño conjunto de medios de "alta tecnología" utilizados por los agresores para acosar, vigilar y controlar a las mujeres en línea y mediante el empleo de las nuevas tecnologías.

Software espía/de acoso y seguimiento por GPS o geolocalización

En una encuesta estadounidense realizada en 70 centros de acogida para víctimas de violencia doméstica, la National Public Radio (NPR) descubrió que "el 85 por ciento de los centros de acogida (habían informado) que trabajaban directamente con víctimas cuyos maltratadores les habían seguido la pista mediante GPS... Unos pocos centros de acogida (dijeron) que los agresores regalaban iPhones a sus hijos e hijas, durante la separación de los padres, con el fin de localizar a la madre" (NPR 2014).

En un reciente estudio francés sobre la prevalencia de la ciberviolencia en el contexto de la violencia doméstica, los investigadores descubrieron que las formas más frecuentes de violencia en línea y facilitada por la tecnología experimentadas por las víctimas eran el "cibercontrol" y el "ciberacoso":[23] seis o siete de cada diez encuestadas habían sido objeto de esos tipos de violencia. Un 29 por ciento de las encuestadas dijo tener la sensación de que su (ex) pareja las había vigilado empleando GPS o un software espía (Centre Hubertine Auclert, 2018). Además, el 41 por ciento de las exparejas de las víctimas habían intentado ponerse en contacto con ellas para humillarlas, acosarlas o controlarlas a través del teléfono de sus hijos e hijas (ibíd.).

El software espía (*spyware*) es un software o una aplicación empleada para seguir la pista de "otra persona convirtiendo su teléfono inteligente, tableta u ordenador en un espía" (NPR 2014). "Diseñadas para ser instaladas en el dispositivo móvil de otra persona, las aplicaciones de software espía (...) se consideran "software de acoso" en el contexto del abuso por parte de la pareja íntima y del abuso basado en el género. ... Además de ese tipo de software, existe una serie de aplicaciones concebidas para la vigilancia de los hijos e hijas y para el control de los empleados que suelen ser utilizadas para controlar a la pareja íntima."[24] Accesibles en las tiendas de aplicaciones a un coste anual que no supera los 200 dólares estadounidenses, esas aplicaciones pueden instalarse en cualquier teléfono inteligente con unas pocas manipulaciones técnicas (instalación de aplicaciones de terceros). Esas aplicaciones permiten al agresor controlar o acosar directamente a la víctima; penetrar y vigilar el teléfono de la víctima; acceder a las comunicaciones de la víctima, y conocer su paradero.

23. Datos recogidos de 212 encuestadas.
24. Guzmán, L., Datos Responsables (2019), "Abordar el acoso y el abuso de género a través de la ley de protección de datos", disponible en: https://responsibledata.io/rd-reflection-stories/addressing-stalkerware-and-gender-based-abuse-through-data-protection-law/.

El agresor tiene acceso al historial de navegación; los mensajes de texto; los correos electrónicos; las llamadas; las redes sociales; los medios como vídeos y fotos; las contraseñas, incluidas las contraseñas de cuentas bancarias y la localización de la víctima en tiempo real mediante GPS.

Desde un punto de vista jurídico, la penalización de esos tipos de abuso varía de un país a otro. Algunos consideran que el cibercontrol y la vigilancia mediante el empleo de programas espía constituye una violación de las comunicaciones privadas y de la intimidad en general. Por ejemplo, esos delitos han sido tipificados así en Francia. Con todo, sólo en contados casos se toman en cuenta las circunstancias agravantes en el contexto de la violencia doméstica. Francia ha actualizado recientemente su ley en materia de violencia doméstica para incluir, entre otras cosas, la vigilancia mediante GPS (Legifrance, 2020). En España, el acceso al teléfono móvil de una pareja o amigo sin su consentimiento está tipificado en el artículo 197 del Código Penal como delito de descubrimiento y revelación de secretos.

Las sanciones impuestas en estos casos son penas de prisión de tres a cinco años. Esas penas pueden aumentarse si se trata de una relación íntima (hasta cinco años de prisión).[25] El Código Penal de Alemania contiene un apartado sobre el acoso (artículo 238.2) que toma en cuenta ese aspecto:

> "Intentar establecer contacto con la otra persona por medio de las telecomunicaciones u otros medios de comunicación o a través de terceros", 238.3. "Utilizar indebidamente los datos personales de la otra persona con el fin de a) encargar bienes o servicios para esa persona, o b) inducir a terceros a ponerse en contacto con esa persona" y 238 4. "Amenazar a la otra persona, a uno de sus familiares o a alguien cercano con causar daños a la vida, la integridad física, la salud o la libertad. (Código Penal de Alemania 1998/2019).

Por lo general, la opinión pública considera ciberdelito toda violación del teléfono o del ordenador de una persona con el empleo de una aplicación o un programa informático como un virus, un malware o un troyano. Europol ha adoptado la misma posición respecto de la instalación de software de acoso en los aparatos de la víctima; con todo, en esos marcos jurídicos el contexto de la violencia doméstica no se considera circunstancia agravante (Europol s.f.).

Las disposiciones del Convenio de Estambul sobre el acoso se aplican tanto al acoso en línea como al facilitado por la tecnología; el Convenio tipifica como delito de acoso "el hecho, cuando se cometa intencionadamente, de adoptar, en varias ocasiones, un comportamiento amenazador contra otra persona que lleve a ésta a temer por su seguridad". Asimismo, incluye una disposición sobre la violencia psicológica para tipificar como delito "el hecho, cuando se cometa intencionadamente, de atentar gravemente contra la integridad psicológica de una persona mediante coacción o amenazas". Las circunstancias agravantes establecidas en los apartados a, b, c, d y h del artículo 46 podrían aplicarse también al acoso cometido en línea o con el empleo de medios digitales. Por otra parte, en las situaciones de peligro para la vida que impliquen el uso de esas herramientas tecnológicas, podría aplicarse también el artículo 52 sobre Órdenes urgentes de prohibición:

> Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las autoridades competentes dispongan de la facultad de ordenar, en situaciones de peligro inmediato, que el autor del acto de violencia doméstica abandone la residencia de la víctima o de la persona en peligro por un período de tiempo determinado y de prohibir que el agresor entre en el domicilio de la víctima o de la persona en peligro o contacte con ella. Las medidas adoptadas de conformidad con el presente artículo deberán dar prioridad a la seguridad de las víctimas o personas en peligro.

Amedrentar, amenazar y controlar por medio del Internet de los objetos (IoT)

En 2020, había ya 50.000 millones de dispositivos conectados en todo el mundo, como los electrodomésticos automatizados y las herramientas domésticas inteligentes que permiten controlar diferentes dispositivos en el hogar, como los termostatos, las bombillas, los mandos a distancia o los altavoces de música inalámbricos. Otros ejemplos de dispositivos conectados son los automóviles; las cámaras de seguridad; los drones domésticos; los monitores de bebés; los dispositivos médicos inteligentes empleados para vigilar la actividad física o la inyección de medicamentos, como las bombas de insulina; los dispositivos corporales [*wearables*] como los Fitbit, los cascos conectados, los relojes o las gafas de realidad virtual, etc. Todos esos instrumentos y aparatos tienen en común el hecho de que están conectados a Internet y que, por tanto, pueden ser activados y controlados a distancia.

25. Código Penal de España, disponible en: www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

El análisis jurídico identifica cuatro tipos de lagunas jurídicas respecto de la Internet de los objetos: cuestiones de discriminación implícita; cuestiones de privacidad; fallas de seguridad, y necesidad de consentimiento (Peppet, 2014). Aunque las cuestiones de discriminación, privacidad y consentimiento afectan a las mujeres de manera específica, en este estudio se examinarán solamente los problemas estructurales de la seguridad de los aparatos e instrumentos de la Internet de los objetos que representan un peligro para las mujeres cuando son empleados como medio de acoso y hostigamiento en el contexto de la violencia doméstica.

La investigación sobre el impacto del acoso, el control y el abuso facilitados por la Internet de los objetos en el contexto de la violencia doméstica está apenas en sus comienzos. Con todo, según algunas previsiones, para 2030 habrá 125.000 millones de instrumentos y aparatos conectados a la Internet de los objetos (Markit, 2017). Por lo tanto, existe una necesidad cada vez mayor de tomar en cuenta esos tipos de violencia y el empleo de los instrumentos y dispositivos del Internet de los objetos a la hora de obtener datos y penalizar la violencia doméstica.

Una investigación del *New York Times* en la que participaron 30 víctimas de violencia doméstica, abogados y abogadas, trabajadores de centros de acogida y personal de emergencia reveló que:

> Una mujer había encendido su aire acondicionado, pero dijo que luego se había apagado sin haberlo tocado. Otra dijo que los números del código de la cerradura digital de su puerta de entrada cambiaban a diario y que no podía comprender a qué se debía. Otra le dijo a una línea de ayuda contra el maltrato que el timbre de la puerta sonaba continuamente, pero que no había nadie... Los agresores utilizan aplicaciones en sus teléfonos inteligentes, que comunican con los dispositivos conectados a Internet para controlar a distancia los objetos de uso cotidiano en el hogar --a veces para vigilar y escuchar a la víctima y otras veces para atemorizarla o demostrar su poder. Los dispositivos solían permanecer en el hogar incluso después de la partida de la pareja, que los seguían utilizando con el fin de intimidar y confundir.

Por consiguiente, no es necesaria la presencia física del agresor para que éste pueda seguir conectado a su víctima y ejercer control, coacción y abuso. Por lo que se refiere a la víctima, el hecho de que puede ser observada y vigilada constantemente y de que los objetos que la rodean pueden contribuir a su sensación de privación de libertad y a sus dificultades físicas, económicas y emocionales puede tener un tremendo impacto psicológico causante de ansiedad, depresión e incluso psicosis, y que puede llevar al suicidio. En efecto,

> Las cerraduras conectadas a Internet pueden restringir los movimientos en determinadas habitaciones, o incluso impedir que alguien salga de su casa. Los asistentes virtuales controlados por la voz pueden informar acerca de todas las preguntas que se le han planteado y del historial de búsquedas ... Asimismo, esos sistemas suelen requerir una cuenta de administración, por lo que una sola persona en un hogar tiene una forma protegida por contraseña para controlar el sistema. (BBC, 2020)

Por lo tanto, es imprescindible que la industria tome en cuenta las cuestiones relativas a la seguridad y la protección de la intimidad desde la etapa de diseño, y también que garantice que en la concepción de esos objetos e instrumentos se tome en cuenta el interés de los usuarios más vulnerables. Con todo, según la Dra. Leonie Tanczer, Profesora de Seguridad Internacional y Tecnologías Emergentes y Directora del proyecto *Gender and IoT* (#GIoT):[26]

> Los medios técnicos no bastan para resolver los problemas sociales. Además, es necesario que en el diseño de esos sistemas participen los servicios oficiales, como las fuerzas del orden, los responsables políticos y los centros educativos, así como las organizaciones de mujeres y los centros de acogida, que deberán ser conscientes de esos riesgos. (Morrow, 2019).

Disposiciones aplicables del Convenio de Budapest

Los artículos del Convenio de Estambul relativos al acoso y a las circunstancias agravantes presentados anteriormente pueden verse reforzados por un conjunto de disposiciones del Convenio de Budapest. Algunas de las disposiciones que se enumeran a continuación tienen una relación más directa con la violencia contra las mujeres en línea y facilitada por la tecnología y el ciberacoso en particular, mientras que otras disposiciones sustantivas penalizan actos que podrían estar vinculados con el ciberacoso, pero la relación es menos directa

26. Género e Internet de los objetos: www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot.

(Consejo de Europa, 2018c). Tales actos podrían facilitar la violencia y podrían llevar a acciones judiciales; con todo, las disposiciones presentadas a continuación no bastarían por sí solas para penalizar la violencia descrita.

Artículo 2 del Convenio de Budapest (Acceso ilícito)

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegitimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Por lo tanto, el acceso a los instrumentos digitales de la víctima (ordenador, tableta o teléfono o aparatos conectados) con el empleo de software de acoso o mediante piratería informática puede ser interpretado en el marco de esa disposición. En el Informe explicativo del Convenio, el "acceso ilícito" se define de la siguiente manera:

> Las amenazas peligrosas y los ataques a la seguridad (es decir, contra la confidencialidad, la integridad y la disponibilidad) de los sistemas y datos informáticos... El término "acceso" abarca la entrada a un sistema informático o a alguna parte del mismo (hardware, componentes, datos almacenados del sistema instalado, directorios, datos relativos al tráfico y datos relacionados con los contenidos).

Artículo 3 del Convenio de Budapest (Interceptación ilícita)

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Esa disposición describe la interceptación sin derecho de los datos personales (no públicos) de una víctima, ya sea mediante la instalación en sus dispositivos de software destinado a interceptar esos datos, o mediante el empleo de medios técnicos que permitan penetrar en sus dispositivos. De hecho, en el Informe explicativo del Convenio de Budapest se explica que:

> La interceptación por "medios técnicos" se refiere a escuchar, monitorear o vigilar el contenido de las comunicaciones, a adquirir los contenidos de datos, ya sea en forma directa, mediante el acceso y uso del sistema informático, o en forma indirecta, mediante el uso de dispositivos electrónicos para escuchar en forma secreta o de dispositivos para intervenir conversaciones. La interceptación puede implicar también la grabación.

Por lo tanto, ese artículo tiene una conexión con la facilitación del ciberacoso, ya que penaliza actos que podrían estar implicados en ese tipo de violencia, pero que en sí mismos no serían suficientes para la penalización del ciberacoso en todas sus dimensiones.

Artículo 4 del Convenio de Budapest (Ataques a la integridad de los datos)

> 1) Cada Parte adoptara las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos. 2) Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

En el contexto de la violencia doméstica, como un ejemplo de esa forma de abuso podríamos poner el caso de una pareja o ex pareja abusiva que destruye o elimina las herramientas, dispositivos o contenidos de la víctima por afán de poder o deseos de venganza. La noción de "daño grave" debe entenderse en el contexto más amplio de la violencia doméstica y debe ser siempre una circunstancia agravante. Ese artículo tiene una conexión tanto directa como con la facilitación de la violencia, similar a la del artículo 5 que se examina a continuación (ya que los ataques a la integridad de los datos pueden causar la muerte o lesiones tanto físicas como psicológicas).

Artículo 5 del Convenio de Budapest (Ataques a la integridad del sistema)

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

En el caso de las tácticas de acoso implicadas en la violencia doméstica, la interferencia y la destrucción, sin derecho, de los datos de una víctima por parte de un agresor, podría estar comprendida en esas dos disposiciones. El "daño grave" resultante de esa acción y la "obstaculización grave" deberán valorarse atendiendo a sus consecuencias para la víctima en el ámbito de la violencia doméstica.

Artículo 6 del Convenio de Budapest (Abuso de los dispositivos)

> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos: a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio; ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a. del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

Esta disposición reviste especial interés por lo que se refiere al software de acoso, cuando el agresor posee "un elemento... con la intención de utilizarlo para cometer los delitos descritos anteriormente, como el acceso y la intromisión ilegales y la interferencia de sistemas y datos" (Consejo de Europa, 2001a).

Formas de violencia psicológica en línea y facilitada por la tecnología

Los tipos de violencia descritos anteriormente también pueden guardar relación con la violencia psicológica. El Convenio de Estambul describe la violencia psicológica como "el hecho, cuando se cometa intencionadamente, de atentar gravemente contra la integridad psicológica de una persona mediante coacción o amenazas". Asimismo, el Informe explicativo del Convenio define la violencia psicológica:

> El ámbito de aplicación del delito se limita a las conductas intencionadas que, por diversos medios y métodos, socavan y dañan gravemente la integridad psicológica de una persona. El Convenio no define lo que constituye un daño grave. Para que la conducta quede comprendida en esta disposición, debe utilizarse la coacción o las amenazas. ... Esta disposición se refiere al comportamiento y no a un hecho puntual. Su objetivo es captar el carácter delictivo de los comportamientos violentos que se producen a lo largo del tiempo, dentro o fuera de la familia. (Consejo de Europa, 2011b).

Todas las formas de violencia contra las mujeres en línea y facilitada por la tecnología tienen repercusiones psicológicas y podrían clasificarse como violencia psicológica ejercida en línea y facilitada por la tecnología. De hecho, las características específicas de la violencia contra las mujeres en línea y facilitada por la tecnología enumeradas en el primer capítulo aumentan las repercusiones para las víctimas. Por otra parte, los autores de la violencia doméstica pueden hacer un uso inapropiado de las tecnologías digitales para intensificar la gravedad de la violencia psicológica de que es objeto la víctima (véanse las secciones sobre el acoso sexual y el acoso en línea). Boukemidja (2018) añade lo siguiente acerca de estas formas de violencia:

> En cuanto a la violencia psicológica, ésta consiste en denigrar, humillar y degradar a la mujer en su valor humano. Se manifiesta mediante ataques verbales, insultos, escenas de celos, amenazas, presiones, chantajes; control de sus actividades; aislamiento de sus familiares, amigos y del mundo exterior. ... El maltrato verbal consiste en la repetición constante de palabras insultantes o injuriosas hacia una mujer. ... El maltrato verbal puede provocar una serie de problemas de comportamiento, emocionales y físicos.

En este contexto, el maltrato verbal implica el uso de palabras hirientes o humillantes como, por ej., poner un apodo ridículo, insultar a la mujer, hacer comentarios racistas o hacerla objeto de burlas constantemente.

La incitación al suicidio o a las autolesiones mediante el uso de las comunicaciones digitales es otro fenómeno que va en aumento; sus repercusiones se ven intensificadas por el anonimato de que disfrutan los autores de violencia en línea, la perdurabilidad de los contenidos y la facilidad para reunir a un gran número de compinches para cometer un ataque masivo contra la víctima. Los ataques en línea, a veces en sitios web dedicados y en las redes sociales pueden llevar a las víctimas a autolesionarse e incluso al suicidio. Las niñas son más propensas a autolesionarse que los varones (Morgan et al., 2017). Por consiguiente, las etiquetas específicas (*dedicated hashtags*) en las redes sociales pueden llevar a chicas vulnerables a autolesionarse para obtener visibilidad o aumentar el número de sus seguidores (BBC, 2019b).

CAPÍTULO 6.

DISPOSICIONES PERTINENTES DE LOS CONVENIOS DE ESTAMBUL Y BUDAPEST

Los cuatro pilares del Convenio de Estambul, a saber, prevención, protección, enjuiciamiento y políticas coordinadas, constituyen la especificidad del enfoque global e integral adoptado en el Convenio. Esos pilares permiten a las Partes formular un conjunto exhaustivo de mecanismos de respuesta a todos los aspectos de la violencia contra las mujeres y la violencia doméstica.

A continuación se presentan comentarios y análisis de las disposiciones del Convenio de Estambul cuando ello sea pertinente para la plena comprensión del fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología. En el comentario se incluirán las disposiciones del Convenio de Budapest cuando éstas puedan complementar de modo eficiente el Convenio de Estambul. Esto se aplica esencialmente a las disposiciones del Convenio de Budapest en materia de derecho procesal y cooperación internacional.

Políticas integradas

Políticas globales y coordinadas (Artículo 7)

El artículo 7 dispone que:

> 1. Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para adoptar y poner en práctica políticas nacionales efectivas, globales y coordinadas, incluyendo todas las medidas pertinentes para prevenir y combatir todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio, y ofrecer una respuesta global a la violencia contra las mujeres;
>
> 2. Las Partes velarán por que las políticas mencionadas en el apartado 1 pongan los derechos de la víctima en el centro de todas las medidas y se apliquen por medio de una cooperación efectiva entre todas las agencias, instituciones y organizaciones pertinentes;
>
> 3. Las medidas tomadas... deberán implicar, en su caso, a todos los actores pertinentes como las agencias gubernamentales, los parlamentos y las autoridades nacionales, regionales y locales, las instituciones nacionales de derechos humanos y las organizaciones de la sociedad civil.

Las políticas efectivas, globales y coordinadas que las Partes deberán adoptar para prevenir y responder a la violencia contra las mujeres también deberán tener en cuenta de manera integral las formas de acoso en línea y facilitadas por la tecnología, el acoso y la violencia psicológica.

La respuesta integral a esa violencia requiere la actualización periódica de las iniciativas de prevención y del marco normativo, tanto civil como penal, para tener en cuenta los tipos específicos e incipientes de violencia contra las mujeres en línea y facilitada por las nuevas tecnologías, especialmente en el ámbito de la violencia doméstica (incluidos los niños y niñas como víctimas o testigos de la violencia en el hogar) o cuando esos tipos de violencia están dirigidos contra grupos de mujeres que ya se ven afectadas por amenazas interseccionales.

Los órganos de gobierno nacionales y locales y las instituciones jurídicas, sociales y de salud deberán contar con suficientes recursos financieros y humanos para responder a esas formas de violencia, en particular para promover el diálogo interinstitucional y para establecer mecanismos de seguimiento y evaluación que permitan verificar los avances y los efectos de las políticas y las iniciativas coordinadas entre organismos y sectores.

Recursos financieros (Artículo 8)

> Las Partes dedicarán recursos financieros y humanos adecuados para la correcta aplicación de políticas integradas, medidas y programas dirigidos a prevenir y combatir todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio, incluidos los que realicen las organizaciones no gubernamentales y la sociedad civil.

La prevención, protección y adecuada respuesta a las formas de violencia contra las mujeres en línea y facilitada por la tecnología requieren disponer de suficientes recursos financieros y humanos a nivel nacional y local. Asimismo, deberán estar disponibles recursos financieros y humanos para la coordinación intersectorial a nivel nacional y local.

Debe alentarse la elaboración de presupuestos claros, transparentes, pertinentes y sensibles a las cuestiones de género en los que estén claramente definidas las sumas asignadas específicamente a la prevención, protección y enjuiciamiento de todas las formas de violencia contra las mujeres. Por consiguiente, esos presupuestos también deberían incluir la asignación de recursos para dar una respuesta integral a las formas de acoso en línea y facilitadas por la tecnología, y a la violencia psicológica que afectan a las víctimas y a sus familiares a cargo. Asimismo, deberían asignarse recursos financieros y humanos a la tarea de obtención de datos y a la investigación sobre esos tipos de violencia (véase también el artículo 11 del Convenio de Estambul).

Organizaciones no gubernamentales y sociedad civil (Artículo 9)

> Las Partes reconocerán, fomentarán y apoyarán, a todos los niveles, el trabajo de las organizaciones no gubernamentales pertinentes y de la sociedad civil que sean activas en la lucha contra la violencia contra las mujeres y establecerán una cooperación efectiva con dichas organizaciones.

Las organizaciones de la sociedad civil, las organizaciones de derechos de la mujer y las organizaciones no gubernamentales han sido responsables tradicionalmente de gran número de iniciativas de respuesta destinadas a las víctimas de la violencia de género contra las mujeres, iniciativas que en muchos casos siguen estando a cargo de esas organizaciones. A pesar de que en muchos países pueden recibir financiación pública, la seguridad financiera de esas organizaciones y la calidad y cantidad de los servicios destinados a las víctimas se ven amenazadas muchas veces por la escasez de recursos, la falta de oportunidades de financiación a largo plazo o los cambios en el panorama político, entre otras cosas.

Por lo tanto, los marcos y programas de respuesta de las organizaciones responsables de luchar contra la violencia doméstica y otras formas de violencia que afectan a las mujeres deberían contar con financiación adecuada que les permitan dar respuesta también a las formas de acoso en línea y facilitado por la tecnología, y a la violencia psicológica. Debe fomentarse un mayor nivel de cooperación, consulta y gobernanza entre este sector y los organismos públicos responsables de la protección de los derechos de las mujeres con el fin de promover la creación y el mantenimiento del mayor número posible de iniciativas de respuesta, y la cooperación con las mismas. Cabe destacar, en particular, las medidas de prevención, como las campañas de sensibilización, la obtención de pruebas y los mecanismos de investigación y protección de las víctimas de la violencia contra las mujeres en línea y facilitada por la tecnología, específicamente en los casos de violencia doméstica, y en los casos de amenazas entrelazadas.

Órgano de coordinación (Artículo 10)

> 1) Las Partes designarán o crearán una o varias entidades oficiales responsables de la coordinación, aplicación, seguimiento y evaluación de políticas y medidas tomadas para prevenir y combatir todas las formas de violencia incluidas en el presente Convenio. Estas entidades coordinarán la recogida de datos a que se refiere el artículo 11, y analizarán y difundirán los resultados.
>
> 2) Las Partes velarán por que las entidades designadas o creadas con arreglo al presente artículo reciban informaciones de naturaleza general relativas a las medidas tomadas conforme al capítulo VIII.
>
> 3) Las Partes velarán por que las entidades designadas o creadas con arreglo al presente artículo tengan capacidad para comunicar directamente y fomentar relaciones con sus homólogos de las otras Partes.

Es importante la creación de órganos de coordinación específicos para abordar todos los aspectos del fenómeno de la violencia de género contra las mujeres, en todos los sectores. Asimismo, es importante que su mandato incluya no sólo la violencia contra las mujeres fuera de línea, sino también las formas de violencia en línea y facilitadas por la tecnología. Para cumplir su cometido pueden apoyarse en los observatorios nacionales u otros mecanismos encargados de la recogida de datos y de la vigilancia de la violencia contra las mujeres en línea y facilitadas por la tecnología. Las observaciones de cada una de las Partes podrían contribuir a establecer instrumentos de referencia que permitan evaluar el progreso y comparar la situación de los derechos de las mujeres y la seguridad de las mujeres en línea, haciendo uso también de las nuevas tecnologías.

Recogida de datos e investigación (Artículo 11)

El artículo 11 dispone que las Partes se comprometen:

> a recoger los datos estadísticos detallados pertinentes, a intervalos regulares, sobre los asuntos relativos a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio; a apoyar la investigación en los ámbitos relativos a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio, con el fin de estudiar sus causas profundas y sus efectos, su frecuencia y los índices de condena, así como la eficacia de las medidas tomadas para aplicar el presente Convenio; .... a realizar encuestas basadas en la población, a intervalos regulares, para evaluar la amplitud y las tendencias de todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio; .... a proporcionar las informaciones recogidas ... al grupo de expertos, ... con el fin de estimular la cooperación internacional y permitir una comparación internacional, ... y a velar por que las informaciones recogidas con arreglo al presente artículo se pongan a disposición del público.

La recogida de datos desglosados y la investigación revisten especial importancia cuando se trata de nuevas formas de violencia que tienen lugar en línea o están mediadas por la tecnología. De hecho, como se señaló al categorizar los tipos de violencia en el marco del Convenio de Estambul, algunas formas de acoso requieren definiciones específicas y un análisis exhaustivo con el fin de diferenciarlas de otros tipos de violencia que no presentan un componente de género. La recogida de datos es esencial para comprender el contexto de la violencia con vistas a orientar la elaboración de políticas y las modificaciones legislativas. Por ejemplo, por lo que se refiere a la violencia doméstica, es especialmente importante registrar la relación entre el autor de la violencia y la(s) víctima(s) y las posibles circunstancias agravantes (número de autores del delito, duración de los abusos, permanencia de los datos, superposición simultánea de varios tipos de violencia, implicación de los hijos y las hijas de la víctima y efectos para ellos, etc.). Asimismo, la obtención de datos sobre las tasas de incidencia y de condena, incluidos los datos de la justicia civil (como las órdenes de alejamiento), es imprescindible para evaluar las repercusiones a nivel social de esos tipos de violencia y acopiar pruebas para formular políticas eficaces. Los datos sobre suicidios o intentos de suicidio, feminicidios y filicidios podrían incluir información sobre el acoso previo o la violencia psicológica perpetrada con el uso de las nuevas tecnologías, a los fines de la penalización y la evaluación de la prevalencia y el papel de esas formas de violencia en los delitos. Debería alentarse encarecidamente el acceso de la ciudadanía a esos datos con el fin de sensibilizarla acerca de esas formas de violencia.

Los datos sobre el acceso a los centros de acogida, los centros de salud, los centros de recursos para mujeres y los servicios de salud y sociales deberían desglosarse para tomar en cuenta esas formas de violencia en el historial de la víctima y de las mujeres. Debería ser posible preguntar a los niños y las niñas solicitantes de asilo si han sido objeto de esos tipos de violencia antes o durante su viaje.

Asimismo, debería fomentarse la planificación de encuestas, métodos de recogida de datos e iniciativas de investigación para determinar las consecuencias de esos tipos de violencia, con el fin de proceder a su medición, incluido su aspecto financiero, ya que se trata de un paso importante para incluir esos tipos de violencia en los marcos jurídicos generales, tanto a nivel nacional como internacional. En todos los casos, la recogida de datos debería adoptar una perspectiva interseccional a fin de que el desglose sea lo más granular posible.

Todos estos datos deberán ser recogidos y tratados de conformidad con las obligaciones de la Parte con relación a la protección de datos. Además, en lo que respecta a los datos específicos sobre la violencia que tiene lugar en las redes sociales, se debería alentar a las Partes a exigir mayor transparencia y rendición de cuentas a las redes sociales, y también a los registradores de dominios y a los propietarios o administradores de foros, en lo que respecta a la disponibilidad de datos pormenorizados sobre la violencia de que son objeto las mujeres en esas plataformas (Algorithm Watch, 2020; Amnistía Internacional, 2020).

Prevención

Obligaciones generales (Artículo 12)

> 1) Las Partes tomarán las medidas necesarias para promover los cambios en los modos de comportamiento socioculturales de las mujeres y los hombres con vistas a erradicar los prejuicios, costumbres, tradiciones y cualquier otra práctica basada en la idea de la inferioridad de la mujer o en un papel estereotipado de las mujeres y los hombres.
>
> 2) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para prevenir todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio por toda persona física o jurídica.
>
> 3) Todas las medidas tomadas conforme al presente capítulo tendrán en cuenta y tratarán las necesidades específicas de las personas que sean vulnerables debido a circunstancias particulares, y pondrán en su centro los derechos humanos de todas las víctimas.
>
> 4) Las Partes tomarán las medidas necesarias para animar a todos los miembros de la sociedad, en particular los hombres y los niños, a contribuir activamente a la prevención de todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio.
>
> 5) Las Partes velarán por que no se considere que la cultura, las costumbres, la religión, la tradición o el supuesto "honor" justifican actos de violencia incluidos en el ámbito de aplicación del presente Convenio.
>
> 6) Las Partes tomarán las medidas necesarias para promover programas y actividades para la autonomía de la mujer.

Los estereotipos y prejuicios, incluidas las costumbres, la religión y la tradición, o el llamado "honor", son el núcleo del continuo de formas de violencia contra las mujeres propagada en línea. Además, las mujeres con identidades entrelazadas, como las lesbianas, bisexuales y queer, y las mujeres trans, las mujeres negras, las mujeres musulmanas o percibidas como musulmanas, las mujeres migrantes, las mujeres con discapacidades y enfermedades crónicas, las mujeres con dificultades económicas y las niñas menores de 18 años, corren el riesgo específico de ser objeto de estereotipos nocivos que conducen a pautas de violencia en línea y facilitadas por el empleo de nuevas tecnologías. Por consiguiente, las iniciativas destinadas a modificar los estereotipos perjudiciales y promover cambios a nivel de la sociedad que lleven a una mayor igualdad de género tendrán efectos positivos en los comportamientos en línea y fuera de línea. Asimismo, deberían generalizarse las iniciativas y los programas que apoyan el empoderamiento y las representaciones positivas de las mujeres en línea. Esas iniciativas, cuando son numerosas, contribuyen a combatir los estereotipos nocivos que pueden propagarse en las redes sociales y afectar a las mujeres, especialmente a aquellas con vulnerabilidades entrelazadas.

Más allá de los cambios culturales y sociales en el ámbito de la igualdad de género, es crucial que los marcos jurídicos tengan en cuenta todas las formas de violencia contra las mujeres, incluidos los tipos de acoso, violencia psicológica e incitación al odio examinados en apartados anteriores. Si las leyes y reglamentos no se modifican, los nuevos casos de violencia mediada por la tecnología seguirán gozando de impunidad. Además de la evolución jurídica, el papel del sistema judicial es crucial para incorporar la perspectiva de género en las leyes existentes mediante la jurisprudencia.

Por otra parte, es esencial que se adopte una perspectiva interseccional en los proyectos, las iniciativas, los programas, las políticas y las leyes destinadas a prevenir y combatir todas las formas de violencia en línea y

facilitada por la tecnología. La atención deberá centrarse en las víctimas y, en particular, en el diseño de esos mecanismos deberán tomarse en cuenta las vulnerabilidades específicas e interrelacionadas.

Asimismo, los hombres y los niños deberían participar en la lucha contra los estereotipos nocivos y recibir formación, con el fin de fomentar comportamientos positivos en línea como el de "espectador activo", especialmente en ámbitos dominados por los hombres, como las comunidades de videojuegos (Active Bystander UK (s.f.); Glitch UK (s.f.)) o en lo que se refiere a formas específicas de violencia en línea, como los ataques de pandillas y el acoso selectivo. Por otra parte, la generalización de la educación digital podría contribuir a eliminar la posible "captación" de hombres y niños jóvenes por parte de grupos extremistas que operan en línea y que promueven estereotipos negativos sobre las mujeres, e incluso instigan la violencia contra ellas, como la subcultura "incel" (celibato involuntario), que en el pasado ha provocado feminicidios masivos en la vida real y que sigue fomentando a diario actos de violencia que van desde el acoso hasta las agresiones.

Sensibilización (Artículo 13)

> 1) Las Partes promoverán o dirigirán, regularmente y a todos los niveles, campañas o programas de sensibilización, incluso en cooperación con las instituciones nacionales de derechos humanos y las entidades competentes en materia de igualdad, la sociedad civil y las organizaciones no gubernamentales, en particular las organizaciones de mujeres, en su caso, para incrementar la concienciación y la comprensión por el público en general de las distintas manifestaciones de todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio y sus consecuencias en los niños y las niñas, y de la necesidad de prevenirlas.
>
> 2) Las Partes garantizarán la amplia difusión entre el público en general de información sobre las medidas disponibles para prevenir los actos de violencia incluidos en el ámbito de aplicación del presente Convenio.

Deberán fomentarse campañas de sensibilización sobre los diferentes tipos de violencia contra las mujeres en línea y facilitada por la tecnología, en todos los sectores de la sociedad, incluso en la industria durante la concepción de los productos. Asimismo, la ciudadanía deberá tener conocimiento de las leyes que sancionan esas formas de violencia, de los servicios especializados de que pueden valerse las víctimas y de las directrices sobre la manera de combatir esa violencia. Debe darse prioridad a la cooperación con los participantes que operan en la esfera digital de modo que las campañas de sensibilización encuentren eco también en línea.

Educación (Artículo 14)

> 1) Las Partes emprenderán, en su caso, las acciones necesarias para incluir en los programas de estudios oficiales y a todos los niveles de enseñanza material didáctico sobre temas como la igualdad entre mujeres y hombres, los papeles no estereotipados de los géneros, el respeto mutuo, la solución no violenta de conflictos en las relaciones interpersonales, la violencia contra las mujeres por razones de género, y el derecho a la integridad personal, adaptado a la fase de desarrollo de los alumnos.
>
> 2) Las Partes emprenderán las acciones necesarias para promover los principios mencionados en el apartado 1 en las estructuras educativas informales así como en las estructuras deportivas, culturales y de ocio, y en los medios de comunicación.

La educación, incluida la educación digital impartida desde una temprana edad, es cada vez más crucial en nuestras democracias para contrarrestar la desinformación y la información errónea que conducen a la explotación, la manipulación, la polarización política y la desconfianza en las instituciones democráticas. Además, esos empeños deben incluir la educación acerca de los nuevos medios de comunicación y las redes sociales, incluidas las estructuras y características de los mismos que hacen posible la visibilidad de los contenidos extremos y la propagación de la violencia. Asimismo, como ya se ha señalado, el sexismo y la misoginia van a menudo acompañados de contenidos políticos extremistas, teorías conspiratorias y posiciones racistas que, en última instancia, conducen a la difusión tanto de representaciones como de comportamientos nocivos en línea dirigidos contra las mujeres. Se debe conceder máxima importancia no solo a la educación jurídica orientada a hacer frente a la violencia contra las mujeres en línea y facilitada por la tecnología, sino también a la inclusión de la educación digital en los programas de estudios sobre la igualdad entre mujeres y hombres. Ello contribuirá a que se comprenda mejor cómo se desarrollan los estereotipos sobre las mujeres y las niñas en Internet, y también a educar a los usuarios acerca del origen de los contenidos que encuentran en línea y acerca de la manera de eliminar los estereotipos y comportamientos perniciosos.

Formación de profesionales (Artículo 15)

> 1) Las Partes impartirán o reforzarán la formación adecuada de los profesionales pertinentes que traten con víctimas o autores de todos los actos de violencia incluidos en el ámbito de aplicación del presente Convenio, en materia de prevención y detección de dicha violencia, igualdad entre mujeres y hombres, necesidades y derechos de las víctimas, así como sobre la manera de prevenir la victimización secundaria.
>
> 2) Las Partes fomentarán la inclusión en la formación a que se refiere el apartado 1 de una formación en materia de cooperación coordinada e interinstitucional con el fin de permitir una gestión global y adecuada de las directrices en los asuntos de violencia incluidos en el ámbito del presente Convenio.

La obligación de brindar formación a los profesionales reviste suma importancia cuando se trata de prevenir las formas de acoso sexual y de violencia psicológica en línea y facilitada por la tecnología. Como se ha señalado en la sección 1.4, las víctimas encuentran diversos tipos de dificultades cuando intentan obtener reparación por la violencia de que han sido objeto. De hecho, una de las dificultades generales que confrontan las víctimas es la falta de información sobre donde pueden encontrar ayuda, lo que genera en las víctimas un sentimiento de impotencia que acrecienta las consecuencias de la violencia. Las principales dificultades con las que chocan las víctimas son la dificultad de encontrar profesionales capacitados que puedan brindar asesoramiento y la falta de formación de los profesionales de los sistemas de justicia penal y de aplicación de la ley. Es de suma importancia desarrollar las mejores prácticas en materia de formación profesional en los campos social, educativo y de la salud, así como en los sectores de la justicia penal y la aplicación de la ley. En concreto, los profesionales de la justicia penal y las fuerzas del orden deberían recibir una formación inicial que los haga sensibles a las cuestiones de género, así como formación continua durante su carrera profesional que les permita mantenerse al corriente de las leyes más recientes aplicables a esas formas de violencia, a la recogida y protección de las pruebas, incluidas las pruebas electrónicas, y a los procedimientos para tomar declaraciones y reunir los antecedentes de las víctimas sin una ulterior victimización. Por otra parte, los profesionales encargados de la tramitación de los expedientes de asilo de las mujeres deberían recibir una formación con perspectiva de género acerca de las formas de violencia en línea y facilitadas por la tecnología que pueden conducir a la migración forzada, especialmente en el contexto de la violencia doméstica.

Programas preventivos de intervención y tratamiento (Artículo 16)

> 1) Las Partes tomarán medidas legislativas u otras para crear o apoyar programas dirigidos a enseñar a quienes ejerzan la violencia doméstica a adoptar un comportamiento no violento en las relaciones interpersonales para prevenir nuevas violencias y cambiar los esquemas de comportamiento violentos.
>
> 2) Las Partes tomarán medidas legislativas u otras necesarias para crear o apoyar programas de tratamiento dirigidos a prevenir la reincidencia de los autores de delitos, en particular los autores de delitos de carácter sexual.
>
> 3) Al tomar las medidas mencionadas en los apartados 1 y 2, las Partes velarán por que la seguridad, el apoyo y los derechos humanos de las víctimas sean una prioridad y que, en su caso, se creen y apliquen esos programas en estrecha coordinación con los servicios especializados en el apoyo a las víctimas.

Cuando existan mecanismos para la prevención y el tratamiento de los autores de actos de violencia, esos mecanismos deberían enriquecerse mediante una formación, con perspectiva de género, acerca de los tipos de violencia digital y los estereotipos nocivos que los sustentan, así como sobre las estructuras y características tecnológicas que los promueven. Cuando no existan esos mecanismos, deberían formularse planes para su creación que incluyan descripciones de las formas de violencia digital y los efectos específicos de esa violencia, así como módulos sobre el coste y las especificidades de los actos perpetrados en la esfera digital.

Participación del sector privado y los medios de comunicación (Artículo 17)

> 1) Las Partes animarán al sector privado, al sector de las tecnologías de la información y de la comunicación y a los medios de comunicación, respetando la libertad de expresión y su independencia, a participar en la elaboración y aplicación de políticas, así como a establecer líneas directrices y normas de autorregulación para prevenir la violencia contra las mujeres y reforzar el respeto de su dignidad.
>
> 2) Las Partes desarrollarán y promoverán, en cooperación con los actores del sector privado, las capacidades de niños, padres y educadores para hacer frente a un entorno de tecnologías de la información y de la comunicación que da acceso a contenidos degradantes de carácter sexual o violento que pueden ser nocivos.

En el documento "Fomentar la participación del sector privado y de los medios de comunicación en la prevención de la violencia contra las mujeres y la violencia doméstica: Artículo 17 del Convenio de Estambul", publicado por el Consejo de Europa como parte de una colección de documentos que explican las diferentes disposiciones del Convenio de Estambul, se exponen los cuatro pilares que sirven de sustento de las medidas que deberán aplicar los Estados, junto con el sector privado y los medios de comunicación, para prevenir la violencia contra las mujeres: 1) mejorar la formación de los profesionales de los medios de comunicación acerca de las cuestiones relacionadas con la igualdad de género y la violencia contra las mujeres; 2) promover la autorregulación de los medios de comunicación y la regulación de los contenidos discriminatorios y violentos; 3) establecer asociaciones para aumentar la cobertura de los medios de comunicación respecto de la igualdad de género y la violencia contra las mujeres; y 4) promover la cooperación en materia de alfabetización mediática (Consejo de Europa, 2015b).

La función del sector privado, del sector de las tecnologías de la información y la comunicación y de los medios de comunicación es realmente fundamental para garantizar la erradicación efectiva de las formas de violencia contra las mujeres en línea y facilitada por la tecnología en todas las plataformas y en todos los instrumentos en que puede perpetrarse. Las Partes deberán establecer mecanismos de seguimiento para velar por la inclusión efectiva de perspectivas centradas en las víctimas en la concepción de productos inteligentes conectados a la Internet de los Objetos, con el fin de mitigar los riesgos potenciales desde la etapa de diseño. Además, las Partes deberían dar prioridad a la cooperación efectiva con el sector de las TIC, sobre todo mediante los mecanismos de cooperación existentes, como el Código de conducta de la UE para luchar contra la incitación al odio en Internet y la asociación del Consejo de Europa con las empresas digitales en el marco del plan del Consejo de Europa de cooperación con las empresas. Asimismo, se podría adoptar un código de conducta específico sobre la violencia contra las mujeres en línea y facilitada por la tecnología, y también crear observatorios nacionales sobre la violencia contra las mujeres que incluirían programas e iniciativas específicos (Consejo de Europa, 2017b).

Se debe alentar a las plataformas en línea a que adopten los marcos internacionales de derechos humanos, incluidos marcos y normas sobre los derechos de las mujeres, y se las debe inducir a que mejoren su rendición de cuentas en lo que respecta a las iniciativas de prevención y las medidas de reparación disponibles para los usuarios y las víctimas. Una notable iniciativa en este sentido es el ya mencionado Plan del Consejo de Europa de Cooperación con las empresas, que permite a las empresas y a los gobiernos aunar esfuerzos para elaborar políticas basadas en los derechos humanos en la esfera digital. Las Partes deberían insistir especialmente en la transparencia y la disponibilidad de datos granulares sobre cada tipo de violencia contra las mujeres perpetrada en las plataformas en línea.

Asimismo, las Partes deben estimular al sector de las TIC para que sea más inclusivo y aumente sobre todo la presencia de mujeres con identidades entrelazadas que aporten una perspectiva más matizada en la concepción de productos e instrumentos y en la gobernanza de esas empresas.

En cuanto a los medios de comunicación, las Partes deben velar por que éstos respeten los principios de la dignidad humana y prohíban toda discriminación por razón de sexo, así como la incitación al odio y todas las formas de violencia de género contra las mujeres. Por lo que respecta a las formas de violencia en línea, los medios de comunicación deben evitar la difusión de perspectivas de culpabilización de las víctimas. Además, las Partes podrían estimular la aparición de iniciativas intersectoriales entre el sector privado, los medios de comunicación y el sector de las TIC con el fin de combatir todas las formas de violencia contra las mujeres en línea y facilitada por la tecnología. Esas iniciativas deberían centrarse principalmente en la lucha contra los estereotipos y comportamientos perniciosos en línea y facilitados por las nuevas tecnologías dirigidos contra las mujeres y las niñas.

Protección

Para alcanzar el objetivo del Convenio de Estambul, una Europa libre de todas las formas de violencia contra las mujeres y de la violencia doméstica, es necesario que las víctimas puedan acceder a una serie de mecanismos de protección que las Partes tienen la obligación de proporcionar. En lo que respecta a las víctimas de la violencia en línea y facilitada por la tecnología, hay una serie de soluciones que podrían proporcionar protección y apoyo a las víctimas.

Obligaciones generales (Artículo 18)

1) Las Partes tomarán las medidas legislativas u otras necesarias para proteger a todas las víctimas contra cualquier nuevo acto de violencia.

2) Las Partes tomarán las medidas legislativas u otras necesarias, conforme a su derecho interno, para velar por que existan mecanismos adecuados para poner en práctica una cooperación eficaz entre todos

los organismos estatales pertinentes, incluidas las autoridades judiciales, los fiscales, las fuerzas y cuerpos de seguridad, las autoridades locales y regionales, así como las organizaciones no gubernamentales y las demás organizaciones o entidades pertinentes para la protección y el apoyo a las víctimas y testigos de todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio, remitiéndose incluso a los servicios de apoyo generales y especializados a que se refieren los artículos 20 y 22 del presente Convenio.

3) Las Partes velarán por que las medidas tomadas conforme al presente capítulo: se basen en una comprensión fundamentada en el género de la violencia contra las mujeres y la violencia doméstica, y se concentren en los derechos humanos y la seguridad de la víctima; se basen en un enfoque integrado que tome en cuenta la relación entre las víctimas, los autores de los delitos, los niños y las niñas, y su entorno social más amplio; estén dirigidas a evitar la victimización secundaria; estén dirigidas a la autonomía e independencia económica de las mujeres víctimas de violencia; permitan, en su caso, el establecimiento de un conjunto de servicios de protección y apoyo en los mismos locales; respondan a las necesidades específicas de las personas vulnerables, incluso los hijos y las hijas de las víctimas, y sean accesibles para ellos.

4) La prestación de servicios no debe depender de la voluntad de las víctimas de emprender acciones legales ni de testimoniar contra cualquier autor de delito.

5) Las Partes tomarán las medidas adecuadas para garantizar la protección consular u otra, y un apoyo a sus nacionales y a las demás víctimas que tengan derecho a la protección conforme a las obligaciones derivadas del derecho internacional.

Este artículo estipula que las Partes deben diseñar y aplicar leyes y políticas destinadas a evitar nuevas victimizaciones, lo que es especialmente relevante cuando se trata de la violencia en línea y facilitada por la tecnología. Se debe alentar a las Partes a que adopten leyes, o interpreten la legislación existente, de manera que puedan dar respuesta a las amenazas que las mujeres experimentan en línea, y a que velen por que la legislación y la gobernanza nacionales promuevan el mejor diálogo posible, formal e informal, entre los organismos responsables de combatir los delitos en línea y facilitados por la tecnología. Esa respuesta debe tener una perspectiva de género e incorporar las características específicas de esos tipos de violencia. Deberá tomar en cuenta que el abuso puede ocurrir en el ámbito de la violencia doméstica; que puede haber maltratos; que puede ser repetitivo y continuo; que puede haber varios autores de actos de violencia; y que repercute en el modo de vida de la víctima y de las personas a su cargo, que incide en su salud psicológica y a veces en su integridad física. Asimismo, esos mecanismos coordinados de respuesta deberían reflejar el hecho de que las víctimas de la violencia en línea y facilitada por la tecnología pueden ser victimizadas una y otra vez ya que los contenidos delictivos perjudiciales podrían seguir siendo visibles y accesibles en línea.

Información (Artículo 19)

Las Partes tomarán las medidas legislativas u otras necesarias para que las víctimas reciban una información adecuada y en el momento oportuno sobre los servicios de apoyo y las medidas legales disponibles en una lengua que comprendan.

En el contexto de las nuevas e incipientes formas de violencia, como las ya señaladas, la existencia y accesibilidad de la información, tanto jurídica como en materia de protección y apoyo, es fundamental para el porvenir de muchas víctimas. Si no cuentan con esa información, en un idioma que comprendan y en un formato y presentación, tanto en línea como fuera de línea, que contemplen requisitos como el lenguaje de signos, el braille, etc., las víctimas permanecen a menudo en el limbo, sin saber qué hacer y a quién acudir.

Servicios de apoyo generales (Artículo 20)

1) Las Partes tomarán las medidas legislativas u otras necesarias para que las víctimas tengan acceso a servicios que faciliten su restablecimiento. Estas medidas deberían incluir, en caso necesario, servicios como el asesoramiento jurídico y psicológico, la asistencia financiera, los servicios de alojamiento, la educación, la formación y la asistencia en materia de búsqueda de empleo.

2) Las Partes tomarán las medidas legislativas u otras necesarias para que las víctimas tengan acceso a servicios de salud y servicios sociales, que los servicios dispongan de recursos adecuados y que los profesionales estén formados para proporcionar una asistencia a las víctimas y orientarlas hacia servicios adecuados.

Las Partes tienen la obligación de ofrecer servicios de apoyo para las víctimas de la violencia contra las mujeres, incluida la violencia en línea y la facilitada por la tecnología. El asesoramiento jurídico y psicológico reviste suma importancia para las víctimas de estas formas nuevas e incipientes de violencia, para evitar su culpabilización; para proporcionarles medios que les permitan presentar denuncias si están dispuestas a hacerlo; para aportar pruebas, y para encontrar apoyo y protección que facilite su recuperación. En el caso de las formas de acoso y violencia psicológica facilitadas por la tecnología que ocurren en el ámbito de la violencia doméstica, las víctimas y también las personas a su cargo deberían poder disfrutar de los mismos servicios de apoyo y protección previstos para las víctimas de violencia doméstica en que no existe un componente digital. En particular, deberían poder tener acceso a servicios de apoyo y protección que tengan en cuenta la especificidad de ese tipo de victimización, que a veces incluye la imposibilidad de permanecer en el hogar cuando los agresores controlan los aparatos domésticos conectados a Internet. Asimismo, deberían poder recurrir a profesionales capacitados que presten atención a los efectos que pueden tener en su seguridad los software espía o de acoso y el acoso en línea.

Apoyo en materia de denuncias individuales/colectivas (Artículo 21)

> Las Partes velarán por que las víctimas se beneficien de información sobre los mecanismos regionales e internacionales de demandas individuales/colectivas aplicables y del acceso a mecanismos. Las Partes promoverán la puesta a disposición de un apoyo sensible y consciente a las víctimas en la presentación de sus demandas.

Las víctimas de la violencia contra las mujeres en línea y facilitada por la tecnología deben recibir información y orientación acerca de la posibilidad de recurrir a mecanismos de denuncia individuales o colectivos, regionales o internacionales, una vez agotados los instrumentos nacionales.

Servicios de apoyo especializado (Artículo 22)

> 1) Las Partes tomarán las medidas legislativas u otras necesarias para suministrar y adecuar, según un reparto geográfico adecuado, servicios de apoyo especializado inmediatos, a corto o largo plazo, a toda víctima que haya sido objeto de cualquier acto de violencia incluido en el ámbito de aplicación del presente Convenio.
>
> 2) Las Partes suministrarán o adecuarán servicios de apoyo especializados para todas las mujeres víctimas de violencia y sus hijos e hijas.

Este artículo, que complementa el artículo 20, afirma que todas las víctimas deben poder disfrutar de protección y apoyo urgente, incluido asesoramiento acerca de su caso específico. De hecho, las víctimas de la violencia contra las mujeres en línea y facilitada por la tecnología deben poder recibir protección inmediata, especialmente cuando esos delitos ocurren en el ámbito de la violencia doméstica y provocan un sentimiento de inseguridad en la víctima o en las personas a su cargo. Las víctimas deberían recibir protección y apoyo inmediatos cuando el agresor emplea contra ellas geolocalización, coerción y control en línea a través de las redes sociales; cuando recurre a programas de acoso instalados en el teléfono, la tableta o el ordenador de la víctima, o cuando se vale de herramientas tecnológicas, como cerraduras inteligentes u otros dispositivos conectados a la Internet de los objetos. Deberán garantizarse servicios de asesoramiento que cuenten con los recursos humanos, financieros y técnicos necesarios para ofrecer un asesoramiento dedicado y específico a las mujeres y niñas afectadas. En este sentido, algunas organizaciones abogan incluso por "la posibilidad de que las víctimas de acoso en línea o facilitado por la tecnología y/o de violencia psicológica, en casos graves de violencia doméstica/de género que no les permiten escapar del control ejercido por el agresor, tengan la posibilidad de acogerse al cambio de identidad (por ej., el cambio de nombre)".[27]

Guardias telefónicas (Artículo 24)

> Las Partes tomarán las medidas legislativas u otras necesarias para establecer a nivel nacional guardias telefónicas gratuitas, accesibles las 24 horas del día, siete días por semana, para proporcionar a las personas que llamen, confidencialmente y respetando su anonimato, consejos relativos a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio.

27. Entrevista con Floriane Volt y Louise Beriot de "Force Juridique de la Fondation des Femmes" (https://fondationdesfemmes.org/), 24 de septiembre de 2020, traducida por la autora.

En lo que se refiere a la violencia contra las mujeres en línea y facilitada por la tecnología, es de suma importancia que las víctimas puedan acceder a las líneas de ayuda, ya sea por teléfono, por chat o por mensajería instantánea, las 24 horas del día los 7 días de la semana, desde su propio país y desde el extranjero, para recibir asesoramiento acerca del maltrato de que han sido objeto, así como información sobre los primeros pasos que deben dar de inmediato (como conservar pruebas mediante capturas de pantalla o grabaciones) y la manera de encontrar remedios.

Apoyo a las víctimas de violencia sexual (Artículo 25)

> Las Partes tomarán las medidas legislativas u otras necesarias para permitir la creación de centros de ayuda de emergencia para las víctimas de violaciones o de violencias sexuales, apropiados, fácilmente accesibles y en número suficiente, para realizarles un reconocimiento médico y médico forense, un apoyo vinculado al traumatismo y consejos.

En los centros u oficinas de orientación para casos de violencia sexual, debería preguntarse de forma sistemática a las víctimas si en el pasado habían sido objeto de formas de acoso o violencia psicológica en línea y facilitada por la tecnología, a fin de poner de relieve el potencial facilitador de las tecnologías digitales en los casos de violación y violencia sexual. Los servicios asistenciales que ofrecen asesoramiento inmediato o a más largo plazo deberían estar equipados para brindar ayuda y apoyo en el caso de experiencias como la violación filmada, en reconocimiento del elemento adicional de trauma y victimización que ello puede conllevar.

Protección y apoyo a los niños testigos (Artículo 26)

> 1) Las Partes tomarán las medidas legislativas u otras necesarias para que, en la oferta de servicios de protección y apoyo a las víctimas, se tengan en cuenta adecuadamente los derechos y necesidades de los niños y niñas testigos de todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio.
>
> 2) Las medidas tomadas con arreglo al presente artículo incluirán los consejos psicosociales adaptados a la edad de los niños y niñas testigos de todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio y tendrán en cuenta debidamente el interés superior del niño.

Este artículo puede complementar **el artículo 31** del Convenio de Estambul **sobre Custodia, derecho de visita y seguridad (Capítulo V, Derecho material).**

Como ya se ha señalado, en muchos casos los teléfonos personales o tabletas de los niños y las niñas se convierten en instrumentos del acoso en línea contra sus madres. Asimismo, durante la cuarentena de la Covid-19, ha aumentado el número de visitas digitales de padres sin custodia. Ese tipo de encuentro conlleva el riesgo de revictimización para las víctimas y sus hijos e hijas, ya que el ex pareja, segundo progenitor o padre abusador puede obtener "pistas sobre la vida de su ex pareja a partir de lo que pueden ver en segundo plano durante las videollamadas y aprovechar esa información para hacer preguntas a los niños y las niñas que podrían poner en peligro la seguridad de sus madres" (Klein, 2020). Los niños y niñas testigos y covíctimas de la violencia deben recibir asesoramiento psicosocial que tenga en cuenta esos riesgos específicos de revictimización. De hecho, el artículo 31 añade que "las Partes tomarán las medidas legislativas u otras necesarias para que, en el momento de estipular los derechos de custodia y visita relativos a los hijos y las hijas, se tengan en cuenta los incidentes de violencia incluidos en el ámbito de aplicación del presente Convenio".

Denuncia y Denuncia por profesionales (Artículos 27 y 28)

> Las Partes tomarán las medidas necesarias para alentar a toda persona testigo de la comisión de cualquier acto de violencia incluido en el ámbito de aplicación del presente Convenio, o que tenga serias razones para creer que se podría cometer algún acto o que hay riesgo de que se produzcan nuevos actos, para que lo denuncie a las organizaciones u autoridades competentes (Artículo 27).
>
> Las Partes tomarán las medidas necesarias para que las normas de confidencialidad impuestas por sus legislaciones internas a ciertos profesionales no impidan, en condiciones apropiadas, hacer una denuncia a las organizaciones u autoridades competentes si tienen razones serias para creer que se ha cometido un acto grave de violencia incluido en el ámbito de aplicación del presente Convenio y que hay riesgo de que se produzcan nuevos actos graves de violencia (Artículo 28).

Por lo que se refiere a las formas de acoso y violencia psicológica en línea tipificadas como delito en su país, los usuarios de las plataformas de Internet deberían poder acceder de inmediato a mecanismos de denuncia tanto en

las plataformas de los proveedores de servicios como en las plataformas policiales. Los profesionales que descubran casos de violencia en línea y facilitada por la tecnología al consultar fuentes de acceso público deberían poder denunciarlos en una plataforma de aplicación de la ley y/o directamente a las fuerzas del orden en una comisaría.

Enjuiciamiento

Las víctimas de violencia en línea y facilitada por la tecnología y sus abogadas o abogados se enfrentan a menudo a numerosos obstáculos a la hora de interponer una acción judicial, o durante el proceso. Algunas dificultades obedecen a la inexistencia de un marco jurídico adecuado para hacer frente a un nuevo tipo de violencia. Otras radican en la falta de formación de los funcionarios del sector de la justicia penal y en la falta de voluntad y de incentivos para recurrir a la jurisprudencia para introducir una perspectiva de género en las leyes vigentes aplicables a la ciberdelincuencia o a los delitos relacionados con la intimidad. El enjuiciamiento efectivo de la violencia contra las mujeres en línea y facilitada por la tecnología se ve dificultado por el reducido número de investigadores especializados que son necesarios para obtener el número de pruebas requerido.

Ciertas dificultades obedecen también a la índole del espacio en línea, al hecho de que gran cantidad de pruebas son ahora electrónicas y a que basta un clic para copiar o distribuir esas pruebas o, por el contrario, borrarlas o modificarlas. Además de los problemas relativos a la admisibilidad de las pruebas electrónicas en los tribunales, la obtención de pruebas cruciales de otro país o de un proveedor de servicios suele resultar muy difícil para las autoridades policiales, si no imposible. Asimismo, las pruebas pueden estar almacenadas en la nube, con los consiguientes problemas de jurisdicción.

> Dado que... la delincuencia en el mundo físico implica cada vez más pruebas electrónicas, el estado de derecho se ve amenazado no sólo en el ciberespacio, sino también en el mundo físico. En última instancia, esa disminución de la capacidad de investigación y de defensa de la seguridad pública y de los derechos humanos se traducirá en vigilantismo o en un mayor número de víctimas que no obtienen justicia.[28]

Existen múltiples marcos jurídicos que regulan, o rechazan, el acceso a las pruebas electrónicas. Como ejemplo cabe mencionar la *Cloud Act*, la ley estadounidense que regula el acceso a las pruebas electrónicas almacenadas en Estados Unidos. Debido a la complejidad de los procedimientos entre los Estados, entre las Partes de los acuerdos internacionales, entre las Partes y los Estados que no son Partes, y entre los Estados y las empresas, a la mayoría de las víctimas les resulta sumamente difícil obtener los resultados apetecidos. El próximo Segundo Protocolo Adicional al Convenio de Budapest contempla abordar algunos de esos problemas relativos al acceso a las pruebas electrónicas y la cooperación internacional de conformidad con el estado de derecho y las normas de derechos humanos, y garantizará que los gobiernos cumplan con su obligación de proteger a las personas y sus derechos en el ciberespacio.

La mayor contribución del Convenio de Estambul es el reconocimiento de la violencia de género contra las mujeres como una violencia que afecta a las mujeres por el hecho de serlo. El Convenio de Budapest complementa esa labor brindando a las Partes en ambos Convenios, y a las Partes en el Convenio de Budapest en los casos de doble incriminación, los medios para procesar eficazmente esos delitos. El próximo Segundo Protocolo Adicional al Convenio de Budapest propone acelerar los procedimientos de asistencia mutua en materia penal (que en la actualidad pueden tomar hasta 18 meses). Esto redundará en un acceso más eficiente de las fuerzas del orden a las pruebas electrónicas almacenadas en otra Parte, incluidos los medios de cooperación en situaciones de emergencia, y la cooperación directa entre una Parte y un proveedor de servicios de Internet situado en otra Parte. Asimismo, el Segundo Protocolo facilitará la divulgación de la información sobre el registro de nombres de dominio (lo que a veces es vital para identificar a los autores del delito y aclarar la responsabilidad) y aportará soluciones para algunos problemas planteados en materia de jurisdicción y territorialidad.[29]

Esas iteraciones facilitarán gran número de procedimientos, incluidos los concernientes a las mujeres víctimas.

A continuación se evaluará un conjunto de disposiciones del Convenio de Estambul relativas a los procedimientos judiciales, complementadas con cláusulas del Convenio de Budapest (cuando proceda) que enriquecen las disposiciones del Convenio de Estambul en relación con la violencia contra las mujeres en línea y facilitada por

28. Comité del Convenio sobre la Ciberdelincuencia (T-CY), Acceso de la justicia penal a las pruebas electrónicas en la nube: Recomendaciones para la consideración del T-CY, Informe final del Grupo de pruebas en la nube del T-CY, 2016, disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.
29. Entrevista con Alexander Seger, Jefe de la División de Ciberdelincuencia y Secretario Ejecutivo del Comité del Convenio sobre la Ciberdelincuencia, septiembre de 2020, www.coe.int/en/web/cybercrime/tcy.

la tecnología. Asimismo, se analizarán otras disposiciones del Convenio de Budapest cuando sean pertinentes para abordar la ciberdelincuencia que afecta a las mujeres por razón de su género.

Investigación, enjuiciamiento, derecho procesal y medidas de protección

En la siguiente sección se evalúa y se hace un comentario sobre la pertinencia de las disposiciones del Convenio de Estambul que guardan relación con el enjuiciamiento de la violencia contra las mujeres en línea y facilitada por la tecnología, complementadas con cláusulas del Convenio de Budapest en materia de investigación y derecho procesal. A continuación, se evalúan las condiciones relativas a la cooperación internacional.

Obligaciones generales (Artículo 49)

> 1) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que la investigación y los procedimientos judiciales relativos a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio se lleven a cabo sin demoras injustificadas, sin perjuicio del derecho de la víctima a todas las fases del proceso penal.
>
> 2) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias, de conformidad con los principios fundamentales de los derechos humanos y teniendo en cuenta la perspectiva de género en este tipo de violencia, para garantizar una investigación y un procedimiento efectivos por los delitos previstos en el presente Convenio.

Esta disposición pone de relieve la importancia de tomar en cuenta la necesidad urgente de enjuiciar todas las formas de violencia contra las mujeres para evitar dar "poca prioridad a las investigaciones y a los procedimientos judiciales, lo que contribuye de manera significativa a un sentimiento de impunidad entre los autores de la violencia y ha contribuido a perpetuar los altos niveles de aceptación de dicha violencia" (Consejo de Europa, 2011b). Esto también es cierto por lo que se refiere a las formas de violencia nuevas e incipientes, como la violencia contra las mujeres en línea y facilitada por la tecnología. Esta disposición también podría servir para "incorporar una perspectiva de género" en el texto del Convenio de Budapest al reconocer la importancia de investigar y enjuiciar la violencia que afecta a las mujeres en línea.

Respuesta inmediata, prevención y protección (Artículo 50)

> 1) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las fuerzas y cuerpos de seguridad competentes respondan de forma rápida y eficaz a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio ofreciendo protección adecuada e inmediata a las víctimas.
>
> 2) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las fuerzas y cuerpos de seguridad competentes tomen de forma rápida y adecuada medidas de prevención y protección frente a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio, incluidas las medidas operativas preventivas y la recogida de pruebas.

Las fuerzas y cuerpos de seguridad deben ser capaces de reaccionar con rapidez y de brindar adecuada protección a las víctimas, así como de participar en iniciativas de prevención y protección, como las medidas operativas preventivas y la recogida de pruebas. Por lo que se refiere a las formas de violencia en línea y facilitadas por la tecnología, el reconocimiento temprano y rápido de ese tipo de violencia por parte de las fuerzas del orden contribuye al establecimiento de procesos óptimos para la recogida de pruebas.

A este respecto, los artículos 16 a 21 del Convenio de Budapest podrían complementar el artículo 50 del Convenio de Estambul en lo que se refiere al enjuiciamiento de la violencia contra las mujeres en línea y facilitada por la tecnología. Asimismo, esos artículos darían a las Partes una orientación más precisa sobre las medidas que deben adoptarse para obtener las pruebas electrónicas en los procedimientos penales en los territorios de las Partes.

Artículo 16 del Convenio de Budapest (Conservación rápida de datos informáticos almacenados)

> 1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2) Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el fin de que las autoridades competentes puedan obtener su revelación. Las Partes podrán prever la renovación de dicha orden.

3) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

El Informe explicativo del Convenio de Budapest destaca que:

> Las medidas contenidas en los Artículos 16 y 17 se aplican a los datos almacenados ya obtenidos y conservados por los titulares de los datos, como, por ej., los proveedores de servicios. ... debido a la volatilidad de los datos informáticos, éstos son fácilmente objeto de manipulaciones y modificaciones. Por lo tanto, valiosas pruebas de un delito pueden desaparecer fácilmente debido a negligencias en el manejo o las prácticas de almacenamiento; a la manipulación o borrado deliberados de los datos con el fin de destruir las pruebas, o a la eliminación sistemática de datos cuya conservación no se requiere por más tiempo. Un método de preservar la integridad de los datos es que las autoridades competentes registren, o accedan de manera similar, y confisquen, o consigan de manera similar, los datos necesarios. ... (los delitos informáticos y los delitos relacionados con el uso de los ordenadores son cometidos en gran medida como resultado de la transmisión de comunicaciones a través de un sistema informático. ... Determinar el origen o el destino de esas comunicaciones pasadas puede contribuir a determinar la identidad de los autores de los delitos. (Consejo de Europa, 2001b).

Artículo 17 del Convenio de Budapest (Conservación y revelación parcial rápidas de los datos relativos al trafico)

1) Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para: a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2) Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

"La obtención de los datos relativos al tráfico almacenados correspondientes a comunicaciones pasadas puede ser esencial para determinar el origen o el destino de las comunicaciones realizadas" (ibíd.). Por lo tanto, este acceso es crucial para identificar a los agresores, incluso si

> En muchos casos no hay ningún proveedor de servicios que posea la suficiente cantidad de datos esenciales relativos al tráfico para poder determinar el origen real o el destino de la comunicación. Cada uno posee una parte del rompecabezas, y es necesario examinar cada una de estas Partes para identificar el origen o el destino de la comunicación ... El artículo 17 garantiza que pueda llevarse a cabo la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de una comunicación. (ibíd.)

Artículo 18 del Convenio de Budapest (Orden de presentación)

1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar: a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

Este artículo es importante, ya que permite a las Partes en investigaciones y procedimientos penales específicos ordenar a una persona que comunique determinados datos informáticos cuando la persona esté presente en el territorio de esa Parte (artículo 18.1a); y ordenar a un proveedor de servicios que comunique los datos relativos a los abonados, cuando el proveedor de servicios ofrezca sus servicios en el territorio de la Parte sin estar necesariamente situado en el territorio (artículo 18.1b).[30] La información sobre el abonado suele ser una pieza clave de información en una investigación penal, ya que puede contener, entre otra información, la dirección IP del presunto autor del delito (o de los autores secundarios).[31] El Segundo Protocolo Adicional establecerá procedimientos para mejorar la cooperación directa con los proveedores y entidades de otras Partes, con sujeción a las salvaguardias adecuadas para tener en cuenta los requisitos únicos que se derivan de la cooperación directa entre las autoridades de una Parte con los proveedores de servicios ubicados en otra Parte.

Artículo 19 del Convenio de Budapest (Registro y confiscación de datos informáticos almacenados)

> 1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar a: a. todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y b. todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.

Ese artículo exige a las Partes la creación de leyes que permitan a las autoridades competentes acceder a los sistemas y servidores informáticos situados en su territorio. "Este artículo tiene como finalidad modernizar y armonizar las leyes nacionales sobre registro y la confiscación de los datos informáticos almacenados con el fin de obtener pruebas relacionadas con investigaciones y procedimientos penales específicos" (Consejo de Europa, 2001b)

Artículo 20 del Convenio de Budapest (Obtención en tiempo real de datos relativos al tráfico)

> 1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes: a. a obtener o grabar con medios técnicos existentes en su territorio; y b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas: i. a obtener o a grabar con medios técnicos existentes en su territorio, o ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

Los datos de tráfico son importantes para las investigaciones, ya que indican el número de visitantes de un sitio web y otros elementos de información de los presuntos sospechosos que se conectan al proveedor de servicios (servidor de correo electrónico, fecha, hora, alias).

> Dichas técnicas a menudo revisten una importancia crucial para la investigación de algunos de los delitos establecidos en el Convenio, tales como los relacionados con el acceso ilícito a sistemas informáticos, y la distribución de virus y de pornografía infantil. Por ejemplo, en algunos casos no es posible determinar la fuente de la intrusión o la distribución sin obtener en tiempo real datos relativos al tráfico. En algunos casos, no es posible descubrir la naturaleza de la comunicación sin la interceptación en tiempo real de los datos relativos al contenido. (ibíd.)

Artículo 21 del Convenio de Budapest (Interceptación de datos relativos al contenido)

> 1) Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno a: a. obtener o grabar con medios técnicos existentes en su territorio; y b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a: i. obtener o grabar con

30. Consejo de Europa, (2017) T-CY Guidance Note #10 on Production orders for subscriber information, disponible en: https://rm.coe.int/16806f943e.
31. "En el curso de una investigación penal, la información sobre los abonados puede ser necesaria principalmente en dos situaciones específicas. En primer lugar, la información sobre el abonado es necesaria para identificar qué servicios y medidas técnicas conexas han sido utilizados o están siendo utilizados por un abonado, como el tipo de servicio telefónico utilizado (por ejemplo, móvil), el tipo de otros servicios asociados utilizados (por ejemplo, desvío de llamadas, correo de voz, etc.), el número de teléfono u otra dirección técnica (por ejemplo, dirección de correo electrónico). En segundo lugar, cuando se conoce una dirección técnica, la información sobre el abonado es necesaria para ayudar a establecer la identidad de la persona en cuestión. Otra información sobre el abonado, como la información comercial sobre los registros de facturación y pago del abonado, también puede ser relevante para las investigaciones penales, especialmente cuando el delito investigado implica fraude informático u otros delitos económicos" (Consejo de Europa 2001b).

medios técnicos existentes en su territorio; o ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

Los datos de contenido son la forma de datos más confidencial, ya que incluyen información como texto, imágenes, fotos, vídeos, sonido, etc. Por tanto, se aplican normas de protección de datos más estrictas que a otras formas de datos. Incluso en el contexto de una investigación penal, "debido al mayor interés por el respeto de la intimidad, tratándose de datos de contenido la diligencia indagatoria se limita a "una serie de delitos graves, que deberá determinar el derecho interno" (ibíd.).

Como ya se ha señalado, los artículos 16 a 21 del Convenio de Budapest son complementarios del artículo 50 del Convenio de Estambul.

Cabe analizar otras disposiciones del Convenio de Estambul en materia de procesamiento penal relacionadas con estos tipos de violencia.

Artículo 51 del Convenio de Estambul (Valoración y gestión de riesgos)

1) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que todas las autoridades pertinentes puedan llevar a cabo una valoración del riesgo de letalidad, de la gravedad de la situación y del riesgo de reincidencia de la violencia a efectos de gestionar el riesgo y garantizar, en su caso, la coordinación de la seguridad y el apoyo.

2) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que la valoración mencionada en el apartado 1 tenga debidamente en cuenta, en todas las fases de la investigación y de la aplicación de las medidas de protección, el hecho de que el autor de actos de violencia incluidos en el campo de aplicación del presente Convenio posea o tenga acceso a armas de fuego.

De hecho, muchas formas de violencia contra las mujeres en línea y facilitada por la tecnología podrían precipitar situaciones potencialmente mortales. Como ya se ha señalado, la violencia sexual puede ir precedida de amenazas y comportamientos de acoso en línea y facilitados por la tecnología. Esto es aún más generalizado en el ámbito de la violencia doméstica. Por lo tanto, las víctimas de violencia doméstica deben disponer de mecanismos coordinados que les brinden apoyo y seguridad, incluso en los casos de abuso perpetrado en línea o facilitado por las nuevas tecnologías.

Artículo 52 del Convenio de Estambul (Órdenes urgentes de prohibición) y Artículo 53 (Mandamientos u órdenes de protección)

Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las autoridades competentes dispongan de la facultad de ordenar, en situaciones de peligro inmediato, que el autor del acto de violencia doméstica abandone la residencia de la víctima o de la persona en peligro por un periodo de tiempo determinado y de prohibir que el autor entre en el domicilio de la víctima o de la persona en peligro o contacte con ella. Las medidas adoptadas de conformidad con el presente artículo deberán dar prioridad a la seguridad de las víctimas o personas en peligro. (Artículo 52)

1) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las víctimas de todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio puedan beneficiarse de mandamientos u órdenes de protección adecuados.

2) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que los mandamientos u órdenes de protección mencionados en el apartado 1: ofrezcan una protección inmediata y no supongan una carga económica o administrativa excesiva para la víctima; tengan efecto por un periodo determinado o hasta su modificación o revocación; en su caso, se dicten sin audiencia a la otra parte y con efecto inmediato; puedan disponerse de forma independiente o acumulable a otros procedimientos judiciales, puedan introducirse en procesos judiciales subsiguientes. (Artículo 53)

Las autoridades que emiten órdenes urgentes de prohibición y de protección deberían ser receptivas a las formas de violencia doméstica perpetrada en línea y facilitada por las nuevas tecnologías. De hecho, las órdenes de prohibición o de protección en muchos casos no mencionan la comunicación electrónica debido a la falta de comprensión por parte de las fuerzas del orden de las numerosas formas de violencia mediadas por las nuevas tecnologías (Asociación para el Progreso de las Comunicaciones/ACNUDH (s.f.)). En algunos países, se conceden excepciones específicamente en cuanto a la comunicación con los niños, incluso por teléfono móvil

o por medios digitales, por lo que las distinciones resultan aún menos nítidas. Además, como los medios de comunicación electrónica se han ampliado y son ahora más variados y menos claros y directos, algunas características de las redes sociales tienen que ver ahora menos con la comunicación (intercambio de mensajes o de contenidos) que con la visualización (ver de forma pasiva el contenido producido por alguien, sin interacción), o incluso a veces con el acoso, por ejemplo, el visualizar las "historias" de alguien en línea o el "orbitar", comportamiento que consiste en no responder a los mensajes de alguien pero seguir observando visiblemente sus contenidos en línea. Por todo ello, resulta aún más difícil establecer una definición clara de lo que constituye contacto entre un agresor y una víctima (Fetters/The Atlantic, 2018).

> Creo que lo que consideramos, y lo que nuestros clientes consideran, ser acciones intimidatorias y acoso no se traduce necesariamente. ... Aunque nuestras clientas se sienten abrumadas y acosadas y que los hechos son obviamente una violación de la orden de protección – por lo que se refiere a la intención de acosar, intimidar y coaccionar – es más difícil establecer que los hechos constituyen realmente una violación desde el punto de vista jurídico (ibíd.).

Artículo 56 del Convenio de Estambul (Medidas de protección)

> 1) Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para proteger los derechos e intereses de las víctimas, incluidas sus necesidades específicas cuando actúen en calidad de testigos, en todas las fases de las investigaciones y procedimientos judiciales, en especial:
>
> a. velando por que tanto ellas como sus familiares y testigos de cargo estén al amparo de los riesgos de intimidación, represalias y nueva victimización;
>
> b. velando por que las víctimas sean informadas, al menos en los casos en que las víctimas y sus familiares podrían estar en peligro, cuando el autor del delito se evada o salga en libertad de forma temporal o definitiva;
>
> c. manteniéndolas informadas, según las condiciones establecidas en su derecho interno, de sus derechos y de los servicios existentes a su disposición, así como del curso dado a su demanda, de los cargos imputados, del desarrollo general de la investigación o del procedimiento y de su papel en el mismo, y de la resolución recaída;
>
> d. dando a las víctimas, de conformidad con las normas procedimentales de su derecho interno, la posibilidad de ser oídas, de presentar elementos de prueba y de exponer sus puntos de vista, necesidades y preocupaciones, directamente o a través de un intermediario, y de que éstos sean examinados;
>
> e. proporcionando a las víctimas una asistencia adecuada para que sus derechos e intereses sean debidamente expuestos y considerados;
>
> f. velando por que se puedan adoptar medidas para proteger la vida privada y la imagen de la víctima;
>
> g. velando por que, siempre que sea posible, se evite el contacto entre las víctimas y los autores de los delitos en la sede de los tribunales o de los locales de las fuerzas y cuerpos de seguridad;
>
> h. proporcionando a las víctimas intérpretes independientes y competentes, cuando las víctimas sean parte en el procedimiento o cuando aporten elementos de prueba;
>
> i. permitiendo a las víctimas declarar ante el tribunal, de conformidad con las normas de su derecho interno, sin estar presente, o al menos sin que el presunto autor del delito esté presente, especialmente recurriendo a las tecnologías de la comunicación adecuadas, si se dispone de ellas.
>
> 2) Se deberán disponer, en su caso, medidas de protección específicas que tengan en consideración el interés superior del menor que haya sido víctima y testigo de actos de violencia contra la mujer y de violencia doméstica.

El artículo 56 es crucial ya que enumera las necesidades de las víctimas en todas las fases del proceso judicial. El tomar en cuenta las necesidades especiales de las víctimas cuando son testigos, y el brindar protección a sus familias y testigos contra la revictimización y las represalias en línea y facilitadas por la tecnología puede eliminar gran número de amenazas vehiculadas por esos medios. A pesar de que su supervisión es generalmente cosa fácil, esos medios pueden tener profundos efectos negativos para las víctimas y sus testigos, lo que a veces entorpece el proceso judicial. Además, se debe tomar en cuenta el papel de las víctimas de la violencia en línea y facilitada por la tecnología a la hora de aportar pruebas, en vista de la especificidad de las pruebas electrónicas (por ejemplo, instantáneas de mensajes, fotos o grabaciones de vídeos ya borrados por el agresor o agresores).

Cooperación internacional

En lo que respecta a la cooperación entre las Partes en el Convenio de Estambul, el artículo 62 estipula que las Partes cooperarán "en la medida más amplia posible" a los fines de "prevenir, combatir y perseguir todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio", así como de "aplicar las sentencias civiles y penales pertinentes, incluidas las órdenes de protección". El Informe explicativo del Convenio explica que las Partes deben "reducir, en la medida de lo posible, los obstáculos a la rápida circulación de información y pruebas" (Consejo de Europa, 2011b).

La cooperación entre las Partes también se aplica cuando una víctima que vive en la jurisdicción de una Parte presenta una denuncia acerca de un delito perpetrado en otra Parte. En el Informe explicativo se explica que "estas autoridades pueden iniciar un procedimiento si su legislación lo permite o transmitir la denuncia a las autoridades del Estado en el que se cometió el delito, de conformidad con las disposiciones pertinentes de los instrumentos de cooperación aplicables a los Estados en cuestión" (ibíd.).

Por último, el Convenio incluye el hecho de que las medidas de asistencia jurídica mutua también pueden encontrar un fundamento en el Convenio de Estambul, aunque los Estados no hayan firmado otro tratado centrado específicamente en la asistencia jurídica mutua, lo que estimula la cooperación jurídica entre las Partes en el Convenio.

En lo referente a la cooperación internacional, la asistencia jurídica mutua y el acceso a las pruebas electrónicas en entornos transfronterizos, los artículos 25 y 29 a 35 del Convenio de Budapest aportan información complementaria.

Artículo 25 del Convenio de Budapest (Principios generales relativos a la asistencia mutua)

> 1) Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.
>
> 3) Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

El Informe explicativo explica que "la obligación de cooperar se aplica, en principio, tanto a los delitos penales relacionados con sistemas y datos informáticos..., como a la obtención de pruebas en formato electrónico de una infracción penal".

En efecto, debido a la volatilidad de los datos electrónicos (fáciles de duplicar o borrar):

> El objetivo del párrafo 3 es, por lo tanto, facilitar la aceleración del proceso de obtención de asistencia mutua de manera tal que la información o las pruebas esenciales no se pierdan debido a que han sido eliminadas antes de que pudiera prepararse, transmitirse y dar respuesta al pedido de asistencia.

Los artículos 29 a 30 del Convenio de Budapest se refieren a la asistencia jurídica mutua en relación con las medidas provisionales.

Artículo 29 del Convenio de Budapest (Conservación rápida de datos informáticos almacenados)

El artículo 29 define las condiciones en las que una Parte puede solicitar a otra Parte la conservación de datos almacenados por medios de sistemas informáticos en el contexto de una investigación penal.[32] Este artículo retoma en el contexto de la cooperación internacional lo dispuesto en el artículo 16 (a nivel nacional) (Consejo de Europa, 2001b).

Como hemos visto, las formas de violencia contra las mujeres en línea y facilitadas por la tecnología están parcialmente cubiertas por los artículos sustantivos 2 a 11 del Convenio de Budapest. Para que la preservación funcione en esos casos, a) las Partes deben aplicar con flexibilidad la doble incriminación; o b) las Partes

32. Los datos informáticos se definen en el Preámbulo del Convenio de Budapest como "toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función".

solicitantes deben pedir la preservación sobre la base de uno de los delitos facilitadores de los artículos 2 a 7 y 11. Por ejemplo, una Parte podría solicitar la preservación en un caso de ciberamenaza basándose en el artículo 2, acceso ilícito al ordenador de la víctima (Consejo de Europa, 2018c).

Artículo 30 del Convenio de Budapest (Revelación rápida de datos conservados)

El artículo 30 es equivalente al artículo 17 (nivel nacional) en el contexto de la cooperación internacional.

Los artículos 31 a 34 abarcan la asistencia mutua en relación con los poderes de investigación.

Artículo 31 del Convenio de Budapest (Asistencia mutua en relación con el acceso a datos almacenados)

El artículo 31 retoma el artículo 19 (nivel nacional) y explica además que una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar a los datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, así como protegerlos y divulgarlos. Deberá darse respuesta a la solicitud lo más rápidamente posible cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación, o cuando los tratados, acuerdos o leyes aplicables prevean una cooperación rápida.

Artículo 32 del Convenio de Budapest (Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público)

El artículo 32 menciona situaciones en las que las fuerzas del orden de una Parte pueden actuar sin autorización de otra en circunstancias limitadas para tener acceso a datos informáticos almacenados si esa Parte obtiene el "consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos" (que podría ser el presunto sospechoso) o cuando son accesibles al público. Con arreglo a la Nota orientativa del artículo 32, "en general, se considera que el personal policial puede acceder a todos los datos disponibles públicamente, y que para ello pueden registrarse o suscribirse a servicios disponibles al público". "Conforme a la Nota Orientativa, se reconoce que las disposiciones del artículo 32 constituyen excepciones al principio de territorialidad, porque permite, sin necesidad de asistencia mutua, el acceso a datos almacenados en el extranjero" (Verdelho, 2019).

Artículo 33 del Convenio de Budapest (Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico)

En virtud del artículo 33, las Partes están obligadas, en el marco de la asistencia judicial mutua y en el contexto de una investigación penal, a recoger datos relativos al tráfico para otras Partes "al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno", para evitar que los proveedores de servicios borren o eliminen datos de tráfico importantes.

Artículo 34 del Convenio de Budapest (Asistencia mutua en relación con la interceptación de datos relativos al contenido)

El artículo 34 define en qué condiciones pueden solicitarse los datos de contenido. Como éstos son el tipo de datos más confidenciales (y están sujetos a las disposiciones sobre protección de la intimidad), esas solicitudes dependen de "los regímenes de asistencia mutua existentes y las leyes nacionales relativas al alcance y la limitación de la obligación de asistencia" (Consejo de Europa, 2001b). Es posible que la legislación nacional vigente de un país no cubra *per se* los delitos en línea y facilitados por la tecnología. En ese caso, para poder brindar su cooperación, el país requerido puede seleccionar elementos de la presentación del país que presentó la solicitud. Por ejemplo, un país podría basarse en el hecho de que se han enviado amenazas, sin tener en cuenta el hecho de que fueron enviadas electrónicamente. Con todo, si la legislación nacional no contempla un delito *per se* y si no se pueden extraer elementos utilizables de una solicitud de asistencia judicial mutua, la cooperación internacional para obtener datos de tráfico o de contenido puede quedar bloqueada (Consejo de Europa, 2018c). No obstante, es importante señalar que los datos de contenido pueden constituir una prueba clave en muchas investigaciones penales, incluso en casos de violencia contra las mujeres.

Como ya se ha señalado, muchas disposiciones de ambos tratados pueden coincidir en lo que concierne al procesamiento de la violencia contra las mujeres en línea y facilitada por la tecnología. Los artículos 16 a 21 del Convenio de Budapest complementan el artículo 50 del Convenio de Estambul en lo que se refiere al acceso y la obtención de pruebas a nivel nacional. Los artículos 25 y 29 a 35 del Convenio de Budapest amplían la capacidad de las Partes en el Convenio de Budapest para conseguir y proteger las pruebas electrónicas, y amplían las facultades de investigación en el contexto de la asistencia jurídica mutua y la cooperación internacional.

CAPÍTULO 7.
OBSERVACIONES FINALES Y RECOMENDACIONES

Observaciones finales

Este estudio se ha centrado en definir el fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología, sus causas y efectos; los puntos en que ocurren esos tipos de violencia, a saber, en todas las plataformas en línea; y los medios empleados, es decir, los instrumentos tecnológicos conectados a Internet controlados por los agresores. La violencia contra las mujeres en línea y facilitada por la tecnología es la perpetuación de las diferentes formas de violencia contra las mujeres que existe fuera de línea, como en la calle, en la oficina, en la escuela y la universidad, en el hogar y en todos los ámbitos de la vida. La mayoría de las formas de violencia contra las mujeres en línea y facilitada por la tecnología ya existían, pero se han ampliado, amplificado y generalizado gracias a Internet, como es el caso de la violencia doméstica, incluidos el abuso y el acoso posterior a la separación.

La violencia en línea y facilitada por la tecnología también tiene una serie de especificidades: la victimización se ve agravada por el número de agresores, la multiplicidad de los canales utilizados, la imposibilidad de escapar y la dificultad para eliminar los contenidos de Internet. Esas características agravan las repercusiones negativas de esa forma de violencia para las víctimas.

Por otra parte, las víctimas se enfrentan a numerosas dificultades para obtener reparación, entre las que destacan la volatilidad de las pruebas y las dificultades experimentadas para encontrar asistencia y asesoramiento. Sigue siendo difícil interponer acciones judiciales, ya que las leyes no van necesariamente a la par de los avances tecnológicos y los funcionarios encargados de hacer cumplir la ley carecen de la formación, los recursos y el equipo necesarios para asesorar a las víctimas.

El Convenio de Estambul es el instrumento de derechos humanos de mayor alcance centrado en la violencia contra las mujeres y la violencia doméstica. Tiene un amplio alcance y abarca todas las formas de violencia contra las mujeres y la violencia doméstica en todos los ámbitos de la vida, por lo que se aplica también a la violencia contra las mujeres y las niñas en línea y facilitada por la tecnología.

El Convenio de Budapest sobre la Ciberdelincuencia y sus protocolos adicionales (el Primer Protocolo Adicional, que abarca el racismo y la xenofobia en línea, y el próximo Segundo Protocolo Adicional, centrados en mejorar la cooperación y la divulgación de pruebas electrónicas en las investigaciones penales) abarcan muchos delitos perpetrados con el uso de un ordenador o contra sistemas informáticos. Las Partes en el Convenio deberán reforzar su derecho procesal penal interno y fortalecer su capacidad en materia de justicia penal para obtener pruebas electrónicas y facilitar de manera eficaz la cooperación internacional y la asistencia judicial mutua en lo tocante a la investigación y el enjuiciamiento de la ciberdelincuencia y otros delitos que entrañen pruebas electrónicas.

Además, el fenómeno es abordado parcialmente también por un gran número de instrumentos internacionales y regionales normativos, entre ellos la Recomendación General nº 35 de la CEDAW; la Recomendación del Consejo de Europa sobre la prevención y la lucha contra el sexismo; la Estrategia de Igualdad de Género; varios artículos de políticas de la UE, incluida la Estrategia de Igualdad de Género de la UE y la Estrategia de la UE sobre los Derechos de las Víctimas; el Reglamento General de Protección de Datos de la UE; la Ley de Servicios Digitales; la Propuesta relativa a las pruebas electrónicas, y varios acuerdos de cooperación como el Código de Conducta de la UE para la lucha contra la incitación ilegal al odio en Internet. Con todo, es necesario lograr una mayor concertación entre esos instrumentos a fin de poder brindar una respuesta integral a las diversas formas de violencia contra las mujeres en línea y facilitada por la tecnología.

El estudio ha establecido una categorización y definiciones de las diferentes formas de violencia contra las mujeres en línea y facilitada por la tecnología y las ha analizado a la luz de los artículos 33, 34 y 40 del Convenio de Estambul, complementados por disposiciones del Convenio de Budapest. Han sido objeto del estudio las formas de acoso sexual que tienen lugar en línea y mediante el empleo de las nuevas tecnologías, como la difusión no consentida de imágenes o vídeos. Este rubro abarca el abuso sexual basado en imágenes; las imágenes rastreras; los ultrafalsos; el exhibicionismo cibernético; las formas de acoso sexual que implican coacción o amenazas, como el sexteo forzado, la sextorsión, las amenazas de violación, el doxeo sexualizado y el ciberacoso escolar sexualizado. Se han analizado las disposiciones de los artículos 3, 8 y 10 del Convenio de Budapest a título complementario. Se han examinado los artículos 2, 3, 5 y 6 del Convenio de Budapest en relación con formas de acoso en línea y facilitado por la tecnología, como la instalación de software espía o de acoso y el abuso facilitado por la Internet de los objetos. Por último, se han abordado formas de violencia psicológica ejercida en línea, incluida la incitación al odio sexista. La expresión del odio sexista se analiza con más detalle en el Apéndice 2 en el contexto de la recomendación del Consejo de Europa sobre la prevención y la lucha contra el sexismo y el Primer Protocolo Adicional al Convenio de Budapest. El análisis de las disposiciones del Convenio de Budapest demuestra que el marco de la ciberdelincuencia puede aplicarse al fenómeno de la violencia contra las mujeres en línea y facilitada por la tecnología, y que las definiciones contenidas en el Convenio sobre la Ciberdelincuencia enriquecen las definiciones de violencia del Convenio de Estambul.

En la última sección se analizaron las aplicaciones de las disposiciones del Convenio de Estambul en materia de políticas integradas, prevención, protección y enjuiciamiento con respecto a esas formas de violencia. Se analizó el artículo 50 del Convenio de Estambul en términos de su relación con los artículos 16 a 21 del Convenio de Budapest, y se examinó el artículo 62 del Convenio de Estambul sobre cooperación internacional a la luz de los artículos 25, 29, 30 y 31 a 34 del Convenio de Budapest.

En conclusión, este estudio ha demostrado que ambos tratados pueden complementarse de forma dinámica. El valor singular del Convenio de Estambul radica en su reconocimiento de la violencia contra las mujeres como violencia que afecta a las mujeres debido a su género y establece claramente que un Estado tiene la obligación de combatirla, incluso recurriendo a los respectivos marcos de justicia penal de las Partes. El Convenio de Budapest aporta importantes elementos en cuanto a las tareas de investigación, obtención de pruebas y cooperación internacional, en relación no solo con los delitos cometidos en línea y facilitados por las nuevas tecnologías, sino también con cualquier delito que implique pruebas electrónicas.

En lo que respecta a la coordinación de políticas y los esfuerzos de prevención y protección, el Convenio de Estambul es crucial para establecer una respuesta decidida ante todas las formas de violencia contra las mujeres. El Convenio de Budapest incluye instrumentos y metodologías de referencia para las Partes que permiten enjuiciar los casos de violencia contra las mujeres en línea y facilitada por la tecnología, incluso en un contexto transfronterizo. Con todo, hasta la fecha, el ámbito de la ciberdelincuencia sigue siendo neutro por lo que se refiere a las cuestiones de género, al punto de que los delitos contra las mujeres perpetrados en línea no están contemplados en los marcos aplicados a la ciberdelincuencia; por lo que se refiere a los ciberdelitos existentes, la perspectiva de género no se ve reflejada en las políticas. Por lo tanto, debido a su

amplio alcance y enfoque integral, el Convenio de Estambul podría servir de base para introducir la perspectiva de género en el campo de la ciberdelincuencia; asimismo, podría servir de modelo para la adopción de políticas sensibles a las cuestiones de género para luchar contra los ciberdelitos que afectan a las mujeres.

Además del diálogo *sensu stricto* entre los instrumentos, a continuación se presenta una serie de recomendaciones.

Recomendaciones

A nivel del Consejo de Europa

- Sería valioso incrementar la cooperación entre el mecanismo de seguimiento del Convenio de Estambul y el T-CY, así como promover una mayor cooperación con la ECRI y otros organismos de lucha contra la discriminación del Consejo de Europa, como el Comité Directivo sobre la antidiscriminación, la diversidad y la inclusión (CDADI).[33] Esa cooperación podría adoptar la forma de un intercambio de puntos de vista y de ideas; por ejemplo, la cuestión de la violencia contra las mujeres en línea y facilitada por la tecnología podría abordarse de una manera mutuamente enriquecedora y complementaria con el fin de conceptualizar una respuesta normalizada.[34]
- Como segundo paso, podrían organizarse actividades de capacitación para las Partes centradas en ambos Convenios con el fin de aumentar el nivel de competencias y la focalización de la respuesta de las Partes en el Convenio de Estambul y de las Partes en el Convenio de Budapest para combatir la violencia en línea y facilitada por la tecnología.

A nivel del Mecanismo de Seguimiento del Convenio de Estambul

- La primera recomendación general del GREVIO, centrada en la dimensión digital de la violencia contra las mujeres, incluye una lista exhaustiva de medidas de orientación para las Partes por lo que se refiere a sus respuestas ante las formas de violencia contra las mujeres en línea y facilitada por la tecnología. En sus procedimientos de evaluación, el GREVIO debería centrar su atención en esas cuestiones.

A nivel de la secretaría del Convenio de Budapest y del T-CY

- El T-CY debería seguir reconociendo la naturaleza de género de la violencia contra las mujeres perpetrada en línea, incluida la ciberdelincuencia de género, en su labor posterior a su Estudio sistemático sobre la ciberviolencia elaborado en 2018;
- El punto focal para la integración de la perspectiva de género designado por la Oficina del Programa de Lucha contra la Ciberdelincuencia (C-PROC) debería garantizar la integración de la perspectiva de género en la conceptualización y ejecución de todas las actividades de cooperación.
- El T-CY podría contemplar la posibilidad de redactar una recomendación general al Convenio de Budapest acerca de la violencia contra las mujeres en línea y facilitada por la tecnología, con vistas a complementar la recomendación general del GREVIO sobre esa cuestión.

A nivel del sector privado

- Se debe alentar a las plataformas a que adopten los marcos internacionales en materia de derechos humanos, incluidos los marcos y normativas sobre los derechos de las mujeres, y a que demuestren una mayor responsabilidad en cuanto a las iniciativas de prevención y reparación disponibles para las víctimas.
- Los Estados deben insistir especialmente en la transparencia y la disponibilidad de datos granulares sobre todo tipo de violencia contra las mujeres perpetrada en esas plataformas.
- Los usuarios de las plataformas de Internet deberían poder acceder a mecanismos directos de denuncia tanto en las plataformas de los proveedores de servicios como en las de las fuerzas del orden; los mecanismos de denuncia deberían tener una perspectiva interseccional.

---

33. La Comisión Europea contra el Racismo y la Intolerancia (ECRI) es un organismo único de vigilancia de los derechos humanos especializado en cuestiones relacionadas con la lucha contra el racismo, la discriminación (por motivos de "raza", origen étnico/nacional, color, ciudadanía, religión, lengua, orientación sexual, identidad de género y características sexuales), la xenofobia, el antisemitismo y la intolerancia en Europa: www.coe.int/en/web/european-commission-against-racism-and-intolerance.
34. Entrevista con el Dr. Gizem Guney, septiembre de 2020.

- Todas las plataformas deberían poner a disposición de los usuarios información jurídica, con arreglo a su país de residencia.
- Las prácticas de moderación deberían tomar en cuenta todas las formas de violencia contra las mujeres perpetrada en línea.
- En lo que respecta a la violencia contra las mujeres facilitada por la Internet de los objetos, los constructores de esos dispositivos deberían aprovechar la experiencia de quienes responden a los casos de violencia doméstica y de las expertas en ciberseguridad e incorporar sus recomendaciones en materia de seguridad en la fase de fabricación.

APÉNDICE 1:

ANÁLISIS DEL ABUSO SEXUAL BASADO EN IMÁGENES COMO UN CIBERDELITO SEXUAL Y DE GÉNERO Y UNA FORMA DE ACOSO SEXUAL EN LÍNEA CON CIRCUNSTANCIAS AGRAVANTES.

Por abuso sexual basado en imágenes se entiende la distribución y difusión no consentida en línea de imágenes o vídeos íntimos, ya sea que hayan sido obtenidos con consentimiento durante una relación romántica o robados o pirateados de los dispositivos de la víctima, lo que a veces va acompañado de tácticas de doxeo.

El abuso sexual basado en imágenes se conoce también como 'explotación sexual basada en imágenes' (Powell y Henry, 2016); 'difusión no consentida de imágenes, vídeos o imágenes íntimas (NCII; véase Facebook (s.f.), por ejemplo); pornografía no consentida (NCP; véase Citron y Franks, 2014) o "pornografía de venganza". De hecho, en muchos estudios se hace hincapié en la necesidad de reemplazar el término "pornografía de venganza", utilizado por los medios de comunicación, con el fin de dar prioridad a la víctima.

En la actualidad, varios autores clasifican esos delitos como una forma de ciberdelincuencia que afecta a las mujeres.

Mary Rogers, por ejemplo, aboga por la inclusión en el Convenio de Budapest del abuso sexual basado en imágenes, y califica ese hecho delictivo como ciberdelito basado en el género. La autora analiza los marcos jurídicos de los Estados Unidos en cuanto a la pornografía no consentida (PNC):

> Los Estados comienzan a incorporar en sus códigos penales leyes sobre PNC, pero el proceso ha sido lento y carece de uniformidad. Para muchas víctimas, el único recurso es la ley de propiedad intelectual, que es un recurso civil y, en la mayoría de los casos, no puede poner freno a la difusión ulterior de una imagen que ya está en línea. Por lo tanto, la inclusión de la PNC en el Convenio proporcionaría una orientación global muy necesaria y fomentaría normativas uniformes en materia de criminalización. (Rogers, 2018)

Miha Šepec, de la Facultad de Derecho de la Universidad de Maribor en Eslovenia, señala la existencia de una relación dialéctica entre los marcos jurídicos respecto de esta cuestión. Algunos países contemplan el abuso sexual basado en imágenes como un delito sexual, mientras que otros lo consideran un delito que afecta a la intimidad de la víctima. En opinión de Šepec, el abuso sexual basado en imágenes es un "ciberdelito relacionado con el contenido", similar a los materiales de pornografía infantil. Como ejemplo, destaca el Código Penal de Eslovenia (2017), que tipifica como delito el abuso sexual basado en imágenes si su difusión afecta gravemente a la intimidad de la persona. Šepec explica que este planteamiento del tema debe: 1) incluir la intención de causar sufrimiento y 2) causar graves perjuicios a la intimidad de la víctima. La autora opina que todo enfoque que no tome en cuenta las innumerables consecuencias que tiene para la víctima el abuso sexual basado en imágenes (por diversión, por fanfarronería, con fines de lucro, etc.) constituye una visión jurídica limitada:

> Muchos autores han propuesto contemplar la pornografía de venganza como violencia sexual facilitada por la tecnología (Henry y Powell, 2016), violencia cibersexual (Cripps y Stermac, 2018), abuso sexual (Citron y Franks, 2014), delito sexual (McGlynn, Rackley y Houghton, 2017) o incluso como "ciberviolación" y que, por lo tanto, lo que se ve atacada es la identidad sexual y la integridad sexual de una persona. Podríamos decir que esa posición es el enfoque moderno, que considera la pornografía de venganza como un delito sexual grave. Por otra parte, la concepción tradicional del derecho penal continental está firmemente anclada en la noción según la cual la pornografía de venganza es un ataque contra el derecho a la intimidad de una persona, su derecho a la dignidad y su buena reputación. Por lo tanto, en la Europa continental, los códigos penales suelen definir la pornografía de venganza como un delito contra la intimidad, la dignidad y la integridad personal de un individuo, es decir, solamente como un delito de violación de la intimidad. Por consiguiente, en esos países el delito no se toma tan en serio como en aquellos en que se considera delito sexual. (Šepec, 2019)

La autora aboga por que, en última instancia, el abuso sexual basado en imágenes se considere "un delito sexual, ya que las consecuencias para la propia integridad sexual guardan mayor relación con las de otros delitos sexuales (especialmente la pornografía infantil o la violencia y el abuso sexuales) que con los delitos contra la intimidad."(Šepec, 2019).

De hecho, muchas Partes en el Convenio de Estambul cuentan con leyes aplicables al abuso sexual por medio de imágenes. Algunas lo consideran un atentado contra la intimidad de la persona, mientras que otras contemplan la dimensión sexual del delito.

- En el Código Penal de Andorra, el abuso está tipificado como delito contra el honor (capítulo IX) o violación de la intimidad (capítulo X).
- En Austria, está contemplado en el derecho penal como "Acoso persistente con sistemas de telecomunicación o informáticos" (artículo 107c) y "Grabaciones de imágenes no autorizadas" (artículo 120a).
- Croacia tipifica como delito la creación, el uso o la difusión de imágenes íntimas en el artículo 144 (Grabación de imágenes no autorizadas) del capítulo XIV del Código Penal, "Delitos contra la intimidad".
- Estonia tipifica como delito la divulgación ilegal de datos personales y la divulgación ilegal de datos personales sensibles en los artículos 157 y 157-1 de su Código Penal. No se hace mención específica a las posibles circunstancias agravantes sexuales y de género cuando afectan a personas mayores de 18 años.
- En Francia, la cuestión cae bajo el artículo 226-2-1 del Código Penal; se considera violación de la intimidad con una dimensión sexual agravante, y el culpable es sancionado con dos años de prisión y una multa de 60 000 euros.
- En Alemania, el artículo 201a del Código Penal contempla la "violación de la intimidad mediante la toma de fotografías u otras imágenes".
- En Polonia, el delito de acoso persistente a otra persona, o a una persona que tiene relaciones estrechas con la víctima, está recogido en el artículo 190a del Código Penal, que incluye también algunas manifestaciones importantes de ese comportamiento en línea. A este respecto, la ley tipifica específicamente como delito la suplantación de identidad en línea con el fin de causar un perjuicio económico o personal a otra persona.
- En Eslovenia se incorporó en el Código Penal el delito específico de acoso que incluye la geolocalización de personas, así como el acoso con el empleo de medios electrónicos de comunicación (artículo 134a).
- En Suiza, la ley no contempla el delito específico de abuso sexual basado en imágenes. El Código Penal contempla el delito de pornografía (artículo 197) o la violación de la intimidad (artículo 179) que tiene en cuenta la dimensión no consentida del delito.
- En España, el artículo 197 del Código Penal, en su versión actualizada, contempla los delitos de descubrimiento y revelación de secretos. La pena tiene en cuenta ese tipo de delitos cuando se producen en el contexto de una (ex) relación íntima.

El marco del Convenio de Estambul, enriquecido por una perspectiva feminista del Convenio de Budapest, permite abordar la cuestión del abuso sexual basado en imágenes como una forma de acoso sexual que se produce en línea y es facilitado por las nuevas tecnologías. Tiene la ventaja de que toma en cuenta la dimensión sexual del delito, la dimensión repetitiva del acoso y las consecuencias para la víctima, ya que el acoso sexual se define como "toda forma de comportamiento no deseado, verbal, no verbal o físico, de carácter sexual, que tenga por objeto o resultado violar la dignidad de una persona, en particular cuando dicho comportamiento cree un ambiente intimidatorio, hostil, degradante, humillante u ofensivo". Al igual que ocurre con otros tipos de violencia que tienen lugar en el ámbito de la violencia doméstica, el Convenio de Estambul permite tipificarla como un delito más grave al incluir, en su conjunto de circunstancias agravantes (artículo 46), el hecho de que "el delito se haya cometido contra un cónyuge o pareja de hecho actual o antiguo, de conformidad con el derecho interno, por un miembro de la familia, una persona que conviva con la víctima o una persona que abuse de su autoridad".

APÉNDICE 2:

ANÁLISIS DE LOS MARCOS EXISTENTES SOBRE EL DISCURSO DE ODIO SEXISTA EN LÍNEA Y LAS RESPUESTAS CONCOMITANTES EN LA LEGISLACIÓN Y EN LA PRÁCTICA DE LAS PLATAFORMAS DE INTERNET

La reciente recomendación del Consejo de Europa sobre la prevención y la lucha contra el sexismo lo define como:

> Cualquier acto, gesto, representación visual, manifestación oral o escrita, práctica o comportamiento, basado en la idea de que una persona o grupo de personas es inferior por razón de su sexo, que tenga lugar en el ámbito público o privado, en línea o fuera de ella, cuyo propósito o efecto sea: vulnerar la dignidad intrínseca o los derechos de una persona o grupo de personas; provocar daño o sufrimiento físico, sexual, psicológico o socioeconómico a una persona o grupo de personas; crear un entorno intimidatorio, hostil, degradante, humillante u ofensivo; constituir un obstáculo a la autonomía y la plena realización de los derechos humanos de una persona o grupo de personas, y preservar y reforzar los estereotipos de género (Consejo de Europa, 2019).

El discurso de odio sexista en línea implica el uso de palabras, insultos, blasfemias y, a menudo, imágenes para comunicar la hostilidad contra las niñas y las mujeres por el hecho de ser mujeres. Los acosadores suelen recurrir a insultos e incluyen comentarios sobre la apariencia física de las mujeres, como su forma o silueta y su conformidad o no con los estereotipos de género y su sexualidad.

La recomendación del Consejo de Europa sobre el sexismo destaca que "internet ha proporcionado un nuevo espacio para la expresión y transmisión del sexismo, especialmente el discurso de odio sexista, a un amplio público, a pesar de que el origen del sexismo no se encuentra en la tecnología, sino en las persistentes desigualdades de género".

El discurso de odio sexista en línea tiene el mismo objetivo que otras formas de discurso de odio, tanto fuera de línea como en línea: disminuir la presencia de una persona en un espacio público, humillarla o ningunearla, imponer su dominación y autoridad, intimidar y atemorizar a una persona para silenciarla y hacerla "invisible".

Un aspecto de la reflexión sobre el discurso de odio sexista en línea es la relación dialéctica entre el discurso de odio y la libertad de expresión.

> Las iniciativas para hacer frente al fenómeno de la violencia contra las mujeres (en línea y facilitada por la tecnología) se han visto frenadas por la yuxtaposición de argumentos de igualdad de género con consideraciones relativas a la libertad de expresión, lo que hasta ahora ha dado como resultado un *statu quo* en el que las mujeres son objeto de violencia y odio en línea, y sus voces son silenciadas, lo que ha sido destacado por los Relatores Especiales de las Naciones Unidas. (Barker y Jurasz, 2019)

Cabe señalar que la cuestión del discurso de odio fue planteada y definida inicialmente en el contexto del racismo y el antisemitismo y que el discurso de odio sexista también tiene un fuerte componente racial. De hecho, la Recomendación nº R (97) 20 del Comité de Ministros del Consejo de Europa sobre el "discurso del odio" lo define como:

> Toda forma de expresión que propague, incite, promueva o justifique el odio racial, la xenofobia, el antisemitismo y cualquier otra forma de odio fundado en la intolerancia, incluida la intolerancia que se exprese en forma de nacionalismo y etnocentrismo agresivo, y de discriminación y hostilidad contra las minorías, los migrantes y las personas de origen inmigrante.

La Recomendación de política general nº 15 de la Comisión Europea contra el Racismo y la Intolerancia (ECRI), de diciembre de 2015, define la incitación al odio como:

> El fomento, la promoción o instigación, en cualquiera de sus formas, del odio, la humillación o el menosprecio de una persona o grupo de personas, así como el acoso, descrédito, difusión de estereotipos

> negativos, estigmatización o amenaza con respecto a dicha persona o grupo de personas y la justificación de esas manifestaciones por razones de "raza", color, ascendencia, origen nacional o étnico, edad, discapacidad, lengua, religión o creencias, sexo, género, identidad de género, orientación sexual y otras características o condición personales.[35]

Por otra parte, el Protocolo Adicional al Convenio del Consejo de Europa sobre la Ciberdelincuencia, relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, exige a los Estados Partes que promulguen la legislación adecuada y garanticen su aplicación efectiva. Además, los Estados deben adoptar legislación y otras medidas que penalicen "la difusión o la puesta a disposición del público de otro modo material racista y xenófobo por medio de un sistema informático" (Consejo de Europa, 2020b).

En su artículo "#MasculinitySoFragile: culture, structure, and networked misogyny", Sarah Banet-Weiser y Kate Miltner (2016) se preguntan "por qué este momento histórico concreto acoge una cepa especialmente virulenta de violencia y hostilidad hacia las mujeres". Según las autoras, esas formas de violencia "no sólo tienen que ver con el género, sino que a menudo también son racistas, y van dirigidas especialmente contra las mujeres de color". Las autoras proponen el concepto de "misoginia en red", y destacan las dimensiones culturales y estructurales que se entrelazan para crear ese nivel de odio en línea contra las mujeres, y específicamente contra las mujeres de color. Algunos grupos propagan esa particular mezcla de sexismo, racismo y violencia; algunos de ellos utilizan la retórica tradicional de extrema derecha para racionalizar la violencia y otros inventan nuevas formas de narrativas de extrema derecha adaptadas a los espacios en línea (Hampton/Slate, 2019; Lavin, 2020).

Esta es una de las razones por las que la autora Margarita Salas se refiere a la relación dialéctica entre el discurso de odio sexista en línea y la libertad de expresión como "la falsa paradoja" y pide que se reconozca el discurso de odio sexista como una forma de violencia similar al racismo y la xenofobia.

> Cuando hablamos de libertad de expresión nos situamos en el paradigma de los derechos humanos. Los derechos humanos son indivisibles, interrelacionados e interdependientes, lo que significa que el avance de un derecho facilita el progreso de los demás, y que la privación de un derecho tiene efectos adversos sobre los demás. Esto significa también que los derechos humanos no deben jerarquizarse, que la libertad de expresión no es más importante que el derecho a vivir una vida exenta de violencia. Asimismo, significa que existen límites legítimos a la libertad de expresión con el fin de lograr un equilibrio con los demás derechos humanos. (Salas/GenderIT, 2013)

El Consejo de Europa viene trabajando desde hace muchos años en el tema de la incitación al odio, habiéndose explorado muchos aspectos, incluida, recientemente, la incitación al odio en línea. "Debido a la proliferación del discurso de odio en línea, se han realizado esfuerzos específicos para comprender su naturaleza peculiar y para hacer frente a sus numerosos desafíos. Aunque la incitación al odio en línea no es intrínsecamente diferente, la naturaleza de los entornos en línea dificulta la asignación de responsabilidades y el desarrollo de medidas jurídicas adecuadas" (Consejo de Europa, 2020b).

Un estudio del Consejo de Europa de 2020 sobre la cuestión del discurso de incitación al odio en línea ha propuesto un modelo de 30 indicadores para la aplicación y evaluación de buenas políticas destinadas a prevenir y combatir el discurso de incitación al odio en línea mediante medidas de protección y de reparación, por ejemplo. Ese estudio destaca que múltiples Partes interesadas fomentan ya *de facto* respuestas al discurso de odio en línea a diferentes niveles como, por ej., en organizaciones internacionales o regionales, en los acuerdos entre Estados y empresas tecnológicas, y en organizaciones de derechos de la mujer y la sociedad civil. Según el autor del estudio, "es correcto que los organismos gubernamentales, las plataformas de Internet y las organizaciones civiles reclamen, y acepten, un reparto equitativo de la carga práctica y de la responsabilidad jurídica que supone hacer frente a la incitación al odio en línea" (Consejo de Europa, 2020a).

Por lo que se refiere a las plataformas de Internet, existen dos tipos de instrumentos para identificar y eliminar el discurso de odio ilegal y el contenido que infringe las políticas de una empresa. Se emplean sistemas destinados a controlar los contenidos de los mensajes, que aplican una lista de reglas y directrices acerca de lo que los usuarios publican (en particular, texto) para determinar si es aceptable o si infringe los términos de servicio de la plataforma (incluida toda infracción de la legislación nacional). Para ello se emplean algoritmos de extracción de texto y aprendizaje automático pero también intervienen moderadores humanos). Las soluciones

35. ECRI (2015), Recomendación de política general nº 15 relativa a la lucha contra el discurso de odio y su Memorándum explicativo, disponible en https://rm.coe.int/ecri-general-policy-recommendation-n-15-on-combating-hate-speech-adopt/16808b7904.

algorítmicas son objeto de muchas críticas (no son lo suficientemente granulares; no prestan atención al contexto; dependen demasiado del conjunto de datos – potencialmente sesgados – empleados para "calibrar" las herramientas o los algoritmos de aprendizaje automático; la responsabilidad es reducida en caso de cuestiones problemáticas, etc.). El empleo de moderadores humanos es también objeto de críticas (malas condiciones de trabajo, ya que estos empleos suelen subcontratarse a países con leyes laborales menos estrictas; formación inadecuada; riesgo de trastornos de estrés postraumático, etc.) (Cambridge Consultants/OfCom, 2019; Sinders, 2017; Breslow, 2018). El contenido se envía más tarde al personal encargado de determinar la conformidad jurídica, que analiza y elimina el contenido ilegal con arreglo a la legislación local.

El segundo mecanismo adoptado por las plataformas de Internet para combatir la presencia del discurso de odio en línea es la impugnación de contenidos. Cada plataforma de redes sociales ofrece un conjunto de medios destinados a responder a las denuncias de incidentes de violencia en línea. Los usuarios deben denunciar los contenidos que infringen las políticas de la empresa o las leyes nacionales en ciertos casos. Los contenidos ilícitos son denunciados también por organizaciones de probada fiabilidad, o por los órganos de supervisión. Algunas plataformas han realizado grandes progresos al respecto, habiendo elaborado páginas que permiten recoger denuncias con todo lujo de detalles e incluyen definiciones de los tipos de violencia y medidas de sensibilización. Otras no han avanzado mucho por lo que a los usuarios les resulta menos fácil denunciar casos de violencia. Cabe señalar que la mayoría de las definiciones de violencia contenidas en las plataformas son neutrales en cuanto al género y distan mucho de incluir un marco interseccional.[36]

Por otra parte, las plataformas están estableciendo estructuras de supervisión, incluidas las consultas públicas sobre las políticas de contenido de las plataformas y las directrices y procesos relativos a la moderación de los contenidos --una forma de supervisión que Alexander Brown ha caracterizado como "el mínimo de lo que podría considerarse supervisión" (Consejo de Europa, 2020a); procesos de apelación internos establecidos a nivel de la plataforma de Internet, utilizados para apelar contra las decisiones de eliminar o no eliminar contenidos; y consejos de supervisión, comités directivos o juntas de supervisión cuyo objetivo es tomar decisiones sobre los casos problemáticos.

En lo que respecta a una respuesta conjunta, coordinada y basada en la autorregulación, por parte del sector privado y de los Estados, cabe mencionar el Código de conducta para combatir la incitación ilegal al odio en línea, adoptado por la Comisión Europea y suscrito por la mayoría de las plataformas de redes sociales (ya mencionado).

Por último, en Europa comienza a aparecer legislación para combatir las formas de incitación al odio en línea. Esos marcos legislativos disponen que las plataformas tienen la obligación de eliminar toda incitación ilegal al odio dentro de plazos específicos (24 horas o siete días, según el tipo de contenido), pero adolecen de una serie de vulnerabilidades inherentes. La legislación sobre la incitación al odio suele prever multas para los casos de incumplimiento reiterado de la obligación de eliminar contenidos en un plazo determinado, por lo que las plataformas prefieren pagar multas en lugar de adaptar sus prácticas. Los especialistas en materia de libertad de expresión señalan los riesgos que lleva aparejado poner las competencias judiciales en manos de actores privados y de permitir que las plataformas tomen decisiones sobre la supresión de la incitación al odio sin un escrutinio externo, o incluso sobre la eliminación de contenidos para evitar responsabilidades, especialmente contenidos específicos como los periodísticos (ibíd.).

De hecho, la actual Ley sobre la Seguridad de la Red (Ley NetzDG) en Alemania, que aborda el discurso de odio ilegal, ha sido objeto de críticas por los especialistas en temas de libertad de expresión y protección de datos ya que la responsabilidad legal que se exige a las plataformas "es problemática porque efectivamente se externalizan poderes cuasi judiciales o de justicia penal a las plataformas de Internet, a pesar de que esas plataformas se caracterizan por carecer de la capacidad y la experiencia necesarias para garantizar los altos niveles de debido proceso que ofrecen los procedimientos judiciales" (ibíd.). Está prevista la actualización en breve de esta Ley.

En Francia, el "proyecto de ley Avia", concebido para obligar a las plataformas a eliminar el discurso de odio "a todas luces ilícito" en un plazo de 24 horas, y suprimir en el plazo de una hora la propaganda terrorista, los materiales señalados como propaganda terrorista o los materiales de abuso sexual de niños y niñas, o de lo contrario enfrentarse al riesgo de ser multadas, fue anulado por el Consejo Constitucional en junio de 2020 por las mismas razones:

36. Véanse, por ejemplo, los centros de ayuda de Facebook (disponible en: www.facebook.com/help/1126628984024935?helpref=hc_global_nav), Twitter (disponible en: https://help.twitter.com/en/rules-and-policies/twitter-report-violation), Snapchat (disponible en: https://support.snapchat.com/fr-FR) y TikTok (disponible en: https://support.tiktok.com/en/).

> Dada la dificultad para determinar dentro del plazo fijado si los contenidos señalados son claramente ilícitos, debido a la sanción en que se incurre a partir de la primera infracción, y en ausencia de una causa específica que exima de responsabilidad, [la legislación] no puede sino incitar a los operadores de plataformas en línea a retirar los contenidos señalados, sean o no manifiestamente ilícitos. (Político, 2020).

Como concluye Alexander Brown, "se recomienda que los organismos estatales, las plataformas de Internet y las organizaciones de la sociedad civil, incluidos los órganos de supervisión, utilicen la sensibilidad hacia las víctimas como indicador o medida del éxito o del progreso de los instrumentos de gobernanza" (Consejo de Europa, 2020a). Por otra parte, la categorización del discurso de odio sexista en el marco del Convenio de Estambul, como una forma de violencia psicológica acompañada de circunstancias agravantes (como, por ejemplo, el número de agresores implicados), podría contribuir a generalizar este enfoque centrado en la legislación de lucha contra el discurso de odio, especialmente cuando se trata de víctimas del discurso de odio sexista e interseccional.

APÉNDICE 3:
GLOSARIO DE TÉRMINOS

Abuso sexual basado en imágenes

El abuso sexual basado en imágenes es la obtención por parte de un agresor de imágenes o vídeos sexualmente explícitos en el curso de una relación, o el pirateo o robo de los mismos del ordenador, las cuentas de redes sociales o el teléfono de la víctima, con el fin de difundirlos en línea.

Airdrop

Airdrop es un servicio creado por Apple que permite a los usuarios intercambiar contenidos con un usuario de otro producto Apple que se encuentre cerca.

Algoritmo

Un algoritmo es un conjunto o secuencia de instrucciones utilizadas para realizar una tarea automatizada en un sistema informático, o para hallar la solución de un problema.

Ataque DDoS (denegación de servicio distribuido)

Un ataque DDoS es un intento de interrumpir el tráfico normal de un servicio o de un servidor abrumándolo con tráfico de Internet.

Ciberacoso escolar [*Cyberbullying*]

El ciberacoso escolar consiste en la intimidación que tiene lugar utilizando herramientas digitales y en entornos digitales, y que suele afectar a los menores.

Desvalorización del cuerpo

La desvalorización del cuerpo implica el avergonzar o burlarse de la apariencia, la forma o el tamaño corporal de alguien.

Dirección IP (dirección de protocolo de Internet)

Una dirección IP es el número asignado a cada uno de los dispositivos conectados a Internet que permite su identificación y localización.

Dispositivos corporales [*Wearables*]

Los dispositivos corporales son dispositivos inteligentes que se llevan en el cuerpo y que recogen, analizan y difunden información física con el fin de monitorear los hábitos o la salud de la persona.

Doxeo [*Doxing*]

El doxeo es el acto de difundir en línea la información personal de una víctima (número de teléfono, dirección de correo electrónico, dirección del domicilio, contacto profesional, etc.), sin su consentimiento, para fomentar el abuso.

Exhibicionismo cibernético [*Cyber flashing*]

El exhibicionismo cibernético consiste en el envío de fotos sexuales no solicitadas empleando aplicaciones de citas, aplicaciones de mensajes o textos, o mediante Airdrop o Bluetooth.

Flamear [*Flaming*]

El flamear (o incendiar) consiste en la publicación de mensajes ofensivos u hostiles, incluidos los insultos, en redes sociales o foros.

Fotos rastreras [*Creepshots*]

Las fotos rastreras son fotos sexualmente sugerentes de mujeres tomadas sin su consentimiento.

Geolocalización

La geolocalización es una función de un dispositivo capaz de deducir su posición geográfica mediante señales GPS o alguna otra característica de conectividad.

Internet de los objetos [*Internet of things*] (IoT por sus siglas en inglés)

La Internet de los objetos es la red de objetos físicos que están conectados entre sí y con Internet, lo que permite el registro y la transmisión de datos sobre su uso.

Levantar la falda [*Upskirting*]

Levantar la falda (o "Falda arriba") consiste en tomar fotos sexuales o íntimas bajo la falda o el vestido de una víctima, sin su consentimiento, a menudo con la intención de difundir ese contenido en línea.

Nube (la)

El término "nube" hace referencia a una forma alternativa de almacenar datos informáticos, en la que los datos digitales no se almacenan en la unidad de almacenamiento físico del usuario, sino en servidores externos, situados a veces en múltiples sitios, propiedad de una empresa de alojamiento y gestionados por ella.

Orbitar [*Orbit*]

"Orbitar" implica no responder a los mensajes de una persona, o no comunicarse directamente con ella, pero seguir observando visiblemente sus contenidos en línea (seleccionar "me gusta", ver historias, etc.).

Pirateo [*Hacking*]

El pirateo es el proceso de entrar en un sistema informático o en una red de forma ilegal o no consentida.

Pruebas electrónicas

Las pruebas electrónicas son todas las derivadas de los datos contenidos o producidos por cualquier dispositivo digital o tecnológico.

Revelar el nombre anterior [*Deadnaming*]

El revelar el nombre anterior es el acto intencionado de llamar a una persona trans por su nombre de nacimiento (que no corresponde a su género) con el fin de avergonzarla, amenazarla, intimidarla o maltratarla.

Sacar del armario [*Outing*]

El sacar del armario consiste en revelar, sin su consentimiento, la orientación sexual o la identidad de género de una persona, a menudo públicamente.

Sexteo [*Sexting*]

El sexteo consiste en el intercambio, envío o recepción de mensajes sexualmente explícitos, a menudo acompañados de fotos o vídeos, mediante mensajes de texto o un chat.

Sextorsión

La sextorsión es el acto de utilizar la amenaza de publicar contenido sexual (imágenes, vídeos, ultrafalsos, rumores sexuales) para amenazar, coaccionar o chantajear a alguien, ya sea para obtener más contenido sexual o reclamar dinero, y a veces ambas cosas.

Software espía [*spyware*] o software de acoso [*stalkerware*]

El software espía es, por lo general, una aplicación descargada en el teléfono o dispositivo de una persona, que se utiliza para monitorear las actividades de ese dispositivo. El software espía se considera sofware de acoso en el ámbito de la violencia doméstica.

Troleo [*Trolling*]

Trolling es el acto de entrar en línea para causar discordia.

Ultrafalsos [*Deepfakes*]

Los ultrafalsos son vídeos en los que un rostro ha sido sustituido a la perfección por otro, utilizando algoritmos y aprendizaje profundo, y manipulando el sonido, para crear la ilusión de que se está mostrando a otra persona.

Videoagresiones [*Happy slapping*]

Las videoagresiones consisten en atacar a una víctima (agresión física o sexual) con el objetivo de grabar la agresión y difundirla en línea.

APÉNDICE 4:
REFERENCIAS

Abdul Aziz Z. (2017), "Due Diligence and Accountability for Online Violence against Women", disponible en: www.duediligenceproject.org.

Active Bystander UK (s.f.), consultado por última vez el 25 de septiembre de 2020, disponible en: www.activebystander.co.uk/.

Agencia de los Derechos Fundamentales de la Unión Europea (2014), "Violence against women: an EU-wide survey. Main results report", disponible en: https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

Ajder H., Patrini G., Cavalli F. y Cullen L. (2019), "The State of Deepfakes: Landscape, Threats, and Impact", disponible en: https://sensity.ai/mapping-the-deepfake-landscape/.

Algorithm Watch (2020), "Our response to the European Commission's planned Digital Services Act", disponible en: https://algorithmwatch.org/en/submission-digital-services-act-dsa/.

Amnistía Internacional (2018), "Toxic Twitter – a toxic place for women", disponible en: www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1.

Amnistía Internacional (2020), "Twitter Scorecard", disponible en: www.amnesty.be/IMG/pdf/20200922_rapport_twitter_scorecard.pdf.

Asociación para el Progreso de las Comunicaciones/ACNUDH (s.f.), "Input on Protection Orders", consultado por última vez el 14 de octubre de 2020, disponible en: www.ohchr.org/Documents/Issues/Women/SR/Shelters/APC_UNSRVAW_input%20on%20protection%20orders.pdf.

Banet-Weiser S. y Miltner K. M. (2016), "#MasculinitySoFragile: culture, structure, and networked misogyny", en *Feminist Media Studies*, disponible en: www.tandfonline.com/doi/full/10.1080/14680777.2016.1120490.

Barker K. y Jurasz O. (2019), "Online Violence Against Women: addressing the responsibility gap?", disponible en: http://eprints.lse.ac.uk/103941/1/WPS_2019_08_23_online_violence_against_women_addressing_the_responsibility_gap.pdf.

BBC (2019a), "Cyber-flashing: 'I froze when penis picture dropped on to my phone'", disponible en: www.bbc.com/news/uk-48054893.

BBC (2019b), "Instagram: Girl tells how she was 'hooked' on self-harm images", disponible en: www.bbc.com/news/uk-47069865.

BBC (2020), "How your smart home devices can be turned against you", disponible en: www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse.

Boukemidja N. B. (2018), "Cyber Crimes against Women: Qualification and Means", en *European Journal of Social Sciences*, disponible en: https://journals.euser.org/files/articles/ejss_v1_i3_18/Boukemidja.pdf.

Breslow J. (2018), "Moderating the 'worst of humanity': sexuality, witnessing, and the digital life of coloniality", disponible en: www.tandfonline.com/doi/full/10.1080/23268743.2018.1472034.

Cambridge Consultants/OfCom (2019), "Use of AI in Online Content Moderation", disponible en: www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf.

CBC (2017), "Aydin Coban sentenced in Dutch court to 10 years for online fraud, blackmail", disponible en: www.cbc.ca/news/canada/british-columbia/aydin-coban-sentenced-netherlands-online-fraud-blackmail-1.4027359.

Centre Hubertine Auclert (2018), "Cyber-violences conjugales", disponible en: www.centre-hubertine-auclert.fr/sites/default/files/documents/rapport_cyberviolences_conjugales_web.pdf.

Childnet/Save the Children/UCLan (2019), Project DeShame, disponible en: www.childnet.com/our-projects/project-deshame.

Citizen Lab (2020), "Installing Fear", disponible en: https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/.

Citron D. y Franks M. A. (2014), "Criminalizing Revenge Porn", disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946.

Código Penal de Alemania (Strafgesetzbuch – StGB) (1998/2019), Código Penal en la versión publicada el 13 de noviembre de 1998 (Boletín Oficial Federal I, pág. 3322), modificado por última vez por el artículo 2 de la Ley de 19 de junio de 2019 (Boletín Oficial Federal I, pág. 844), disponible en: www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

Comisión Europea (2019), "E-evidence - cross-border access to electronic evidence", disponible en: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

Comisión Europea (2020a), Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Una Unión de la igualdad: Estrategia para la Igualdad de Género 2020-2025, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0152&from=ES.

Comisión Europea (2020b), Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Estrategia de la UE sobre los derechos de las víctimas (2020-2025), disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020DC0258&from=ES.

Comisión Europea (2020c), "Countering illegal hate speech online, 5th evaluation, of the Code of Conduct", disponible en: https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf.

Comisión Europea (2020d), Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a un mercado único de servicios digitales (Ley de servicios digitales) y por el que se modifica la Directiva 2000/31/CE, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0825&from=ES.

Comité para la Eliminación de la Discriminación contra la Mujer (2017), Recomendación General nº 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general nº 19, disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2017/11405.pdf.

Consejo de Europa (2001a), Convenio sobre la Ciberdelincuencia, disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf .

Consejo de Europa (2001b), Informe explicativo del Convenio sobre la Ciberdelincuencia, disponible en: https://rm.coe.int/16802fa403.

Consejo de Europa (2003), Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos: https://rm.coe.int/168008160f.

Consejo de Europa (2007), "Trafficking in human beings: Internet recruitment", disponible en: https://rm.coe.int/16806eeec0.

Consejo de Europa (2011a), Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, disponible en: https://rm.coe.int/1680462543 .

Consejo de Europa (2011b), Informe explicativo del Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, Serie de Tratados Europeos del Consejo de Europa nº. 210, disponible en: https://rm.coe.int/16800d383a.

Consejo de Europa (2015a), Comité de las Partes, Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica, Reglas de procedimiento del Comité de las Partes, disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046325b.

Consejo de Europa (2015b), "Encouraging the participation of the private sector and the media in the prevention of violence against women and domestic violence", disponible en: https://rm.coe.int/16805970bd.

Consejo de Europa (2017a), *Journalists under pressure – Unwarranted interference, fear and self-censorship in Europe*, disponible en: https://book.coe.int/en/human-rights-and-democracy/7295-pdf-journalists-under-pressure-unwarranted-interference-fear-and-self-censorship-in-europe.html.

Consejo de Europa (2017b), "Partnership with Digital Companies", disponible en: https://rm.coe.int/leaflet-partnership-with-internet-companies-en/168079ced2.

Consejo de Europa (2018a), *Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data*, disponible en: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

Consejo de Europa (2018b), Consejo de Europa. Estrategia de Igualdad de Género, disponible en: https://rm.coe.int/estrategia-de-igualdad-de-genero-del-coe-es-msg/16808ac960Una.

Consejo de Europa (2018c), "*Mapping study on cyberviolence*", Comité del Convenio sobre la Ciberdelincuencia, Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG), disponible en: https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c.

Consejo de Europa (2019), Recomendación CM/Rec(2019)1 del Comité de Ministros a los Estados miembros para prevenir y combatir el sexismo, disponible en: https://rm.coe.int/def-26-09-19-recomendacion-consejo-de-europa-sexismo/1680981feb .

Consejo de Europa (2020a), Brown A., "Models of Governance of Online Hate Speech. On the emergence of collaborative governance and the challenges of giving redress to targets of online hate speech within a human rights framework in Europe", disponible en: https://rm.coe.int/models-of-governance-of-online-hate-speech/16809e671d.

Consejo de Europa (2020b), Comité de Expertos sobre la lucha contra el discurso de odio, documento de referencia, disponible en: https://rm.coe.int/background-for-adi-msi-dis-june-2020/16809f6b6d.

Consejo de Europa (2020c), "4 Ps Brochure", disponible en: https://rm.coe.int/istanbul-convention-violence-against-women-brochure-4ps-en/16809ecc93.

Consejo de Europa (2020d), Declaración del Presidente y el Vicepresidente del Comité de Lanzarote sobre el aumento de la protección de los niños contra la explotación y el abuso sexual en tiempos de la pandemia de COVID-19, disponible en: https://rm.coe.int/covid-19-lc-statement-en-final/16809e17ae.

Consejo de Europa (2021), Grupo de Expertos en la lucha contra la violencia contra las mujeres y la violencia doméstica, "General Recommendation No.1 on the Digital Dimension of Violence against Women", disponible en: se actualizará después del 24 de nov.

Daskal J. y Kennedy-Mayo D. (2020), "Budapest Convention: What is it and how is it being updated?", Cross-Border Data Forum, disponible en: www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

Dodaj A. y Sesar K. (2020), "Sexting categories", en *Mediterranean Journal of Clinical Psychology*, disponible en: https://cab.unime.it/journals/index.php/MJCP/article/view/2432/0.

Dreßing H., Bailer J., Anders A., Wagner H. y Gallas C. (2014), "Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims", en *Cyberpsychology, Behavior, and Social Networking*, 17(2), págs. 61-67, disponible en: www.few.vu.nl/~eliens/sg/local/cyber/social-stalking.pdf.

European Women's Lobby (2017), "#HerNetHerRights resource pack" disponible en: www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf.

Europol (s.f.), "High-Tech crime, Crime areas", consultado por última vez el 1º de octubre de 2020, disponible en: www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/high-tech-crime.

Facebook (s.f.), "Not without my Consent", www.facebook.com/safety/notwithoutmyconsent/pilot, consultado por última vez el 14 de octubre de 2020.

Fetters A./*The Atlantic* (2018), "Why It's Hard to Protect Domestic-Violence Survivors Online", disponible en: www.theatlantic.com/family/archive/2018/07/restraining-orders-social-media/564614/.

Fondation des Femmes (s.f.), "Une Force Juridique", consultado por última vez el 20 de septiembre de 2021, disponible en: https://fondationdesfemmes.org/une-force-juridique/.

FRA (Agencia de los Derechos Fundamentales de la Unión Europea) (2014), "Violence against women: an EU-wide survey. Main results report", disponible en: https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-repor.

Ging D. y Siapera E. (2018), "Special issue on online misogyny", en *Feminist Media Studies*, disponible en: https://doi.org/10.1080/14680777.2018.1447345.

Glitch UK (s.f.), "A little means a lot", consultado por última vez el 1º de octubre de 2020, disponible en: https://fixtheglitch.org/almal/.

Glitch y End Violence against Women (2020), "The Ripple Effect, Covid-19 and the epidemic of online abuse", disponible en: https://glitchcharity.co.uk/wp-content/uploads/2021/04/Glitch-The-Ripple-Effect-Report-COVID-19-online-abuse.pdf.

Guney G. (2020), "The Group of Experts under the Istanbul Convention on Preventing and Combating Violence against Women and Domestic Violence and the ECtHR: Complementary or Contradictory Tools?", EJIL:Talk!, Blog of the *European Journal of International Law*, disponible en: www.ejiltalk.org/the-group-of-experts-under-the-istanbul-convention-on-preventing-and-combating-violence-against-women-and-domestic-violence-and-the-ecthr-complementary-or-contradictory-tools/.

Hampton R./Slate (2019), "The Black Feminists Who Saw the Alt-Right Threat Coming", disponible en: https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html.

Megarry J. (2014), "Online incivility or sexual harassment? Conceptualising women's experiences in the digital age", en *Women's Studies International Forum*, 47, págs. 46-55, disponible en: www.sciencedirect.com/science/article/abs/pii/S0277539514001332.

Harris B. (2020a), "Technology, domestic and family violence: perpetration, experiences and responses", QUT Centre for Justice, disponible en: https://eprints.qut.edu.au/199781/1/V1_Briefing_Paper_template.pdf.

Harris B. (2020b), "Technology and Violence Against Women", en Walklate S., Fitz-Gibbon K., Maher J. y McCulloch J. (eds.), *The Emerald Handbook of Feminism, Criminology and Social Change* (Emerald Studies in Criminology, Feminism and Social Change), Emerald Publishing Limited, págs. 317-336, disponible en: https://doi.org/10.1108/978-1-78769-955-720201026.

Hinson L., Mueller J., O'Brien-Milne L. y Wandera N. (2018), "Technology-facilitated gender-based violence: What is it, and how do we measure it?", Centro Internacional de Investigaciones sobre la Mujer, disponible en: www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/.

Kelly L. (1988), *Surviving Sexual Violence* (Feminist Perspectives Series), University of Minnesota Press.

Khouiel L./Vice (2020), "Quand le revenge porn s'adapte au confinement", disponible en: www.vice.com/fr/article/bvg4pz/quand-le-revenge-porn-sadapte-au-confinement.

Klein J. (2020), "Virtual parental visitation could have unintended consequences for abuse survivors", en *The Atlantic*, disponible en: www.theatlantic.com/family/archive/2020/06/dangers-virtual-visitation-abuse-victims/613243/.

Langlais-Fontaine C. (2020), "Démêler le vrai du faux : étude de la capacité du droit actuel à lutter contre les deepfakes", en *La Revue des droits de l'homme*, disponible en: http://journals.openedition.org/revdh/9747.

Lavin T. (2020), *Culture Warlords: My Journey Into the Dark Web of White Supremacy*, Hachette, New York.

Laxton C./Women's Aid (2014), "Virtual World, Real Fear, Women's Aid report into online abuse, harassment and stalking", disponible en: http://bit.ly/2h0W4OX.

Legifrance (2018), Loi no. 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, disponible en: www.legifrance.gouv.fr/jorf/id/JORFTEXT000037284450/.

Legifrance (2020), Loi no. 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales, disponible en: www.legifrance.gouv.fr/jorf/id/JORFTEXT000042176652.

Liggett O'Malley R. (2020), "Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime", disponible en: www.researchgate.net/publication/339798771_Cyber_Sextortion_An_Exploratory_Analysis_of_Different_Perpetrators_Engaging_in_a_Similar_Crime.

Maple C., Shart E. y Brown A. (2011), "Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey", University of Bedfordshire, disponible en: www.beds.ac.uk/media/244385/echo_pilot_final.pdf.

Markit I. (2017), "The Internet of Things: A movement, not a market", citado en López-Neira I., Patel T., Parkin S., Danezis G. y Tanczer L. (2019), "'Internet of Things': How abuse is getting smarter", Safe – The Domestic Abuse Quarterly, disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350615.

McGlynn C., Rackley E. y Houghton R. (2017), "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse", disponible en: https://link.springer.com/article/10.1007/s10691-017-9343-2#citeas.

Morgan C., Webb R. T., Carr M. J., Kontopantelis E., Green J., Chew-Graham C. A., Kapur N. y Ashcroft D. M. (2017), "Incidence, clinical management, and mortality risk following self-harm among children and adolescents: cohort study in primary care", en *BMJ 359*, j4351, disponible en: www.bmj.com/content/359/bmj.j4351.

Morrow S. (2019), "Should We Worry About IoT Being Used as a Weapon of Mass Control?", IoTforall, disponible en: www.iotforall.com/iot-domestic-abuse.

NPR (National Public Radio) (2014), "Smartphones Are Used To Stalk, Control Domestic Abuse Victims", disponible en: www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

O'Connell A. y Bakina K. (2020), "Using IP rights to protect human rights: copyright for 'revenge porn' removal", en *Legal Studies*, Cambridge University Press, disponible en: www.cambridge.org/core/journals/legal-studies/article/using-ip-rights-to-protect-human-rights-copyright-for-revenge-porn-removal/2C1840AC0EB870FB2134CEE9586E76D6.

Pariser E. (2011), *The Filter Bubble: What the Internet Is Hiding from You*, Penguin UK.

Parlamento Europeo (2020), "Answer to a Parliamentary question", disponible en: https://www.europarl.europa.eu/doceo/document/E-9-2020-002184-ASW_ES.html

Peppet S. R. (2014), "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074.

Plan International (2020), "Free to be online? A report on girls' and young women's experiences of online harassment", disponible en: https://plan-international.org/publications/freetobeonline.

Politico (2020), "French constitutional court strikes down most of hate speech law", disponible en: www.politico.eu/article/french-constitutional-court-strikes-down-most-of-hate-speech-law/.

Powell A. y Henry N. (2016), "Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives", disponible en: www.researchgate.net/publication/297673926_Policing_technology-facilitated_sexual_violence_against_adult_victims_police_and_service_sector_perspectives.

Powell A., Scott A. J., Flynn A. y Henry N. (2020), "Image-based sexual abuse: An international study of victims and perpetrators", disponible en: www.researchgate.net/publication/339488012_Image-based_sexual_abuse_An_international_study_of_victims_and_perpetrators.

Rogers M. (2018) "No More Revenge: Criminalizing Non-Consensual Pornography Through the Convention on Cybercrime", *Michigan Journal of International Law*, University of Michigan Law School, Ann Arbor, Michigan, disponible en: www.mjilonline.org/no-more-revenge-criminalizing-non-consensual-pornography-through-the-convention-on-cybercrime/.

Salas M./GenderIT (2013), "The false paradox: freedom of expression and sexist hate speech", disponible en: www.genderit.org/es/node/3820.

Salter M., Dragiewicz M., Burgess J., Fernández A., Suzor N., Woodlock D. y Harris B. (2018), "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms", *Feminist Media Studies*, disponible en: www.researchgate.net/publication/323847103_Technology_facilitated_coercive_control_Domestic_violence_and_the_competing_roles_of_digital_media_platforms.

Šepec, M., (2019), "Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence", International Journal of Cyber Criminology, disponible en: https://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf

Servicio de Estudios del Parlamento Europeo (2021), "Combating gender-based violence: Cyber violence, European added value assessment", disponible en: www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf.

Setterfield R. (2019), "The regulation of 'revenge porn' in England and Wales: are existing legal solutions effective?", University of Surrey, disponible en: https://openresearch.surrey.ac.uk/esploro/outputs/doctoral/The-regulation-of-revenge-porn-in/99515640902346?institution=44SUR_INST.

Simonovic D. (2020), Consejo de Derechos Humanos, Relatora Especial sobre la violencia contra la mujer, "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", disponible en: https://digitallibrary.un.org/record/1641160.

Sinders C. (2017), "Current Reading List (of papers) on Online Harassment and Machine Learning", disponible en: https://medium.com/@carolinesinders/current-reading-list-of-papers-on-online-harassment-and-machine-learning-c70fe674f9d1.

Starr T. S. y Lavis T. (2018), "Perceptions of Revenge Pornography and Victim Blame", en *International Journal of Cyber Criminology*, vol. 12, núm. 2, julio-diciembre de 2018, disponible en: www.cybercrimejournal.com/Starr&Lewisvol12issue2IJCC2018.pdf.

UIP (2018), "Sexism, harassment and violence against women in parliaments in Europe", disponible en: www.ipu.org/resources/publications/issue-briefs/2018-10/sexism-harassment-and-violence-against-women-in-parliaments-in-europe.

Unión Europea (2008), Decisión marco 2008/913/JAI del Consejo, de 28 de noviembre de 2008, relativa a la lucha contra determinadas y manifestaciones del racismo y la xenofobia mediante el Derecho penal, disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al33178.

Van der Wilk A. (2018), Policy Department for Citizens' Rights and Constitutional Affairs, "Cyber violence and hate speech online against women", disponible en: www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf.

Verdelho P. (2019), "Obtaining digital evidence in the global world", UNIO – EU Law Journal, disponible en: https://revistas.uminho.pt/index.php/unio/article/view/2298.

Woodlock D. (2017), "The Abuse of Technology in Domestic Violence and Stalking", Violence Against Women, disponible en: http://marvin.cs.uidaho.edu/Teaching/CS112/domesticAbuseStalking.pdf.

El Convenio de Estambul es el tratado internacional más ambicioso para luchar contra la violencia contra las mujeres y la violencia doméstica. Su amplio conjunto de disposiciones cubre medidas preventivas y de protección de gran alcance, así como una serie de obligaciones para garantizar una respuesta adecuada por parte de la justicia penal ante estas graves violaciones de los derechos humanos. El Convenio de Budapest sobre la Ciberdelincuencia es el tratado internacional más relevante sobre la ciberdelincuencia y las pruebas electrónicas. Establece la penalización de los delitos contra y por medio de computadoras, las herramientas de derecho procesal para proteger las pruebas electrónicas y la cooperación internacional entre las Partes.

Este estudio analiza la aplicación complementaria de estos dos convenios para combatir la violencia contra las mujeres en línea y facilitada por la tecnología a través de políticas coordinadas, prevención, protección, enjuiciamiento y cooperación internacional.

PREMS 047722

ESP

www.coe.int

El Consejo de Europa es la principal organización del continente que defiende los derechos humanos. Cuenta con 46 Estados miembros, incluidos todos los miembros de la Unión Europea. Todos los Estados miembros han suscrito el Convenio Europeo de Derechos Humanos, tratado concebido para proteger los derechos humanos, la democracia y el Estado de derecho. El Tribunal Europeo de Derechos Humanos supervisa la aplicación del Convenio en los Estados miembros.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE