PRINCIPALES HERRAMIENTAS CONCEPTUALES Y JURÍDICAS PARA PREVENIR, SANCIONAR Y ERRADICAR LA VIOLENCIA DE GÉNERO CONTRA LAS MUJERES FACILITADA POR LAS TECNOLOGÍAS

EUROsocIAL
PROGRAMA PARA LA COHESIÓN SOCIAL
Financiado por la Unión Europea
OEA | MESECVI

PRINCIPALES HERRAMIENTAS CONCEPTUALES Y JURÍDICAS PARA PREVENIR, SANCIONAR Y ERRADICAR LA VIOLENCIA DE GÉNERO CONTRA LAS MUJERES FACILITADA POR LAS TECNOLOGÍAS

Este documento forma parte de las acciones conjuntas de EUROsociAL, Programa de la Unión Europea para la cohesión social en América Latina durante su fase puente (2023-2024), el Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI) y la Comisión Interamericana de Mujeres (CIM), para aportar insumos a la elaboración de una Ley Modelo para prevenir, sancionar y erradicar la violencia contra las mujeres facilitada por las nuevas tecnologías.

La presente publicación ha sido elaborada con el apoyo financiero de la Unión Europea. Su contenido es responsabilidad exclusiva de los/as autores/as y no necesariamente refleja los puntos de vista de la Unión Europea ni de la Organización de los Estados Americanos.

Dirección general
Ana Pérez Camporeale, Coordinadora del Área de Políticas de Igualdad de Género del Programa EUROsociAL fase puente.

Alejandra Mora Mora, Secretaria Ejecutiva de la Comisión Interamericana de Mujeres (CIM).

Investigación
Dª Adilia de las Mercedes, Jurista especializada en Derechos Humanos, experta EUROsociAL fase puente

Coordinación y asistencia técnica
EUROsociAL fase puente: Sofia Gonzalez Chiraux, Encargada de proyectos, Expertise France.

OEA/CIM/MESECVI: Luz Patricia Mejía Guerrero, Secretaria Técnica del MESECVI; Eva Villarreal Pascual, especialista en género y violencia contra las mujeres; Sara Brochet, especialista; Tatiana Bensa, especialista en comunicaciones.

Diseño y diagramación: Jerem Aspen

Índice

prólogo

El programa de la Unión Europea, EUROsociAL y el Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI) han emprendido un esfuerzo colaborativo, junto con expertas, instituciones públicas, espacios académicos, y organizaciones de la sociedad civil, para la construcción de una Ley Modelo Integral para prevenir, sancionar y erradicar la violencia de género contra las mujeres facilitada por las tecnologías.

El 30 de noviembre y 1 de diciembre 2023, se llevó adelante el evento: "Hacia una Ley Modelo Integral para prevenir, sancionar y erradicar la violencia de género contra las mujeres facilitada por las tecnologías: Herramientas y propuestas para una regulación regional. El Continuum de violencia" para comenzar a dialogar sobre las violencias que experimentan las mujeres en sus interacciones digitales e identificar los temas más relevantes que deberán ser tenidos en cuenta en la elaboración de la mencionada Ley Modelo. Este documento es un aporte a dicho proceso de consensos y aprendizajes.

En 2020[1], se calculó que una de cada dos mujeres jóvenes sufría ciberviolencia basada en el género. Sabemos que las violencias y las desigualdades estructurales constituyen un reto para lograr un desarrollo integrador, igualitario y sostenible. Si las mujeres y niñas no pueden vivir una vida libre de violencia no podrán contribuir al desarrollo de sus países ni disfrutar de una vida plena.

La violencia en línea dirigida a las mujeres supone un obstáculo para el ejercicio libre y pleno de sus derechos fundamentales. El acoso, la intimidación y los insultos en las redes sociales tienen repercusiones profundas en la vida cotidiana de las mujeres y las niñas. De manera cada vez más frecuente, vemos como estas amenazas borran las fronteras entre lo online y lo offline, convirtiendose en agresiones en el plano físico.

La estrategia para la igualdad de género 2020-2025 de la Unión Europea hace mención expresa a la estrecha vinculación entre Violencia "digital" y la participación política: La ciberviolencia afecta especialmente a las mujeres activas en la vida pública, como las políticas, las periodistas y las defensoras de los derechos humanos. Esto puede tener el efecto de silenciar a las mujeres, obstaculizar su participación en la sociedad y socavar el principio de democracia consagrado en el Tratado de la Unión Europea y por lo tanto ir en contra de los valores fundamentales de la UE de impulsar un desarrollo inclusivo y sostenible[2]. Por esta razón, cabe destacar la importancia del compromiso multisectorial, público y privado en alianza para la construcción de tecnologías más seguras donde la prevención y eliminación de la violencia basada en género sea una prioridad.

Por su parte, el Comité de Expertas del MESECVI, en su XIX Reunión en noviembre de 2022, determinó la importancia de avanzar en el desarrollo de herramientas que coadyuven a la adaptación de los marcos normativos en los Estados Parte de la Convención de Belém do Pará, así como a la creación de políticas públicas, que atiendan el creciente impacto de la violencia de género facilitada por las tecnologías. Frente a este diagnóstico, en junio de 2023, CIM/MESECVI lanzó el proceso de elaboración de la Ley Modelo antes mencionada, con el apoyo de una alianza diversa de Estados, agencias internacionales y organizaciones de la sociedad civil.

A 30 años de la Convención de Belém do Pará y ad portas del aniversario de la Plataforma de Beijing, estamos convencidas que la alianza estratégica entre la Unión Europea y América Latina y el Caribe tiene mucho para aportar en la lucha contra las violencias facilitadas por las tecnologías, sobre todo en la promoción de un compromiso multisectorial que logre una profunda transformación cultural.

Este documento constituye un aporte esencial en la ruta hacia la erradicación de estas violencias que perpetúan el continuum de violencias contra las mujeres, al profundizar en los estándares de protección de sus derechos humanos y proveer herramientas conceptuales y jurídicas para prevenir, sancionar y erradicar la violencia de género contra las mujeres facilitada por las tecnologías.

Ana Pérez Camporeale
Coordinadora del Área de Políticas de Igualdad de Género
Programa EUROsociAL Puente

Alejandra Mora Mora
Secretaria Ejecutiva
Comisión Interamericana de Mujeres
Organización de los Estados Americanos (CIM/OEA)

1 Servicio de Estudios del Parlamento Europeo (EPRS), Lucha contra la violencia de género: Ciberviolencia, evaluación del valor añadido europeo, 2021.

2 https://international-partnerships.ec.europa.eu/policies/global-gateway/initiatives-region/initiatives-latin-america-and-caribbean_en

Introducción

La violencia de género facilitada por las tecnologías es la más reciente evolución de las históricas y desiguales relaciones de poder entre hombres y mujeres. Por su especificidad, estas violencias contra las mujeres generan un alto riesgo de victimización reiterada, prolongada, continua y, en muchas ocasiones, pública: factores que refuerzan la creación, normalización y multiplicación de los estereotipos y prejuicios de género en entornos e interacciones digitales. Según diferentes mecanismos internacionales y regionales de derechos de las mujeres,[3] este tipo de violencia ha afectado, al menos en alguna ocasión, a tres cuartas partes de las mujeres alrededor del mundo.[4]

Aunque cualquier mujer es susceptible de ser víctima de la violencia contra las mujeres facilitada por las tecnologías (VCMFT), desde Naciones Unidas, la Organización de Estados Americanos y la Unión Europea[5] se ha detectado que determinadas colectividades se ven particularmente afectadas, entre ellas, las mujeres feministas, activistas LGBTIQ+, artistas, mujeres en cargos públicos y en la política de partidos, periodistas, blogueras, influencers, defensoras de los derechos humanos y otras figuras públicas. Estos grupos soportan, a su vez, en múltiples ocasiones más de un factor de riesgo, como el hecho de pertenecer a una comunidad perseguida o estigmatizada. Tal es el caso, por ejemplo, de las mujeres migrantes, refugiadas, con discapacidad y en otras situaciones específicas de riesgo de exclusión o vulnerabilidad que deben ser analizadas, de acuerdo con el deber internacional de los Estados, desde un enfoque interseccional.

La VCMFT es un escenario de complejidad creciente no solo por la interrelación de las tecnologías actuales en la amplificación y reproducción de las violencias preexistentes sino por el carácter transnacional de estas, a causa de las diferentes nacionalidades de las empresas intermediarias de servicios, de los victimarios y de los Estados en los que se asientan unas y/u otros. Esta naturaleza transfronteriza implica una dimensión multijurisdiccional que facilita la impunidad al complejizar la persecución de los agresores y, peor aún, al dificultar o impedir la protección efectiva de las víctimas y sobrevivientes.

Aún no hay una forma globalmente consensuada de nombrar la mayoría de los hechos y delitos en estos casos. La terminología a utilizar está en continuo desarrollo y en proceso de debate, consenso y fijación en los distintos foros nacionales e internacionales. Conceptos como "violencia en línea", "ciberviolencia", "violencia digital", "violencia facilitada por las tecnologías" o "dimensión digital de la violencia contra las mujeres" son algunos de los más comunes tanto para describir distintas realidades como para tipificar las conductas punibles. En este proceso de nombrar la realidad se han utilizado términos que muchas víctimas han denunciado como revictimizantes; tal es el caso de "sextorsión" o "pornovenganza", por citar solo un par de ejemplos. Así, conceptualizar, nombrar, definir y delimitar la realidad de estas formas de violencia es un complejo debate al que este inventario de estándares internacionales con distintos niveles de exigibilidad pretende contribuir.

En este contexto de acelerada evolución, sin posibilidades de completitud, el presente compilado expone múltiples avances de los Estados y de la comunidad internacional para combatir la VCMFT y garantizar el derecho de las mujeres a una vida libre de violencias. A tal fin, se han organizado temática y analíticamente distintas normas, jurisprudencia, resoluciones, informes y recomendaciones procedentes tanto del Derecho internacional como del Derecho comparado, que evidencian los progresos que se han

3 La Relatora Especial de la ONU sobre la violencia contra la mujer, sus causas y consecuencias, representantes del Comité de la ONU para la Eliminación de la Discriminación contra la Mujer (CEDAW), el Grupo de Trabajo de la ONU sobre discriminación contra mujeres y niñas, el Grupo de Expertas en la lucha contra la violencia contra la mujer y la violencia doméstica (GREVIO), la Relatora sobre los Derechos de la Mujer de la Comisión Interamericana de Derechos Humanos, la Relatora Especial sobre los Derechos de la Mujer en África y el Comité de Expertas del Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI).

4 Plataforma de Mecanismos de Expertos Independientes sobre la Discriminación y la Violencia Digital contra la Mujer (EDVAW), informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022.

5 Organización de Estados Americanos (OEA), Comisión Interamericana de Mujeres (CIM), MESECVI y ONU Mujeres, "informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022, págs. 21-22; Parlamento Europeo, Resolución de 14 del diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia, párrs. H y AC; y Directiva del Parlamento y del Consejo Europeo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 8 de marzo de 2024, Considerando 17.

venido produciendo en la materia, así como la necesidad de un marco regulatorio internacional específico que establezca, entre otros aspectos, una tipología delictiva común o, cuando menos, compatible entre los diferentes Estados, la responsabilidad de las empresas intermediarias de servicios en la prevención y erradicación de los hechos de violencia online y la necesaria coordinación entre los Estados y el resto de agentes concernidos para proporcionar una protección efectiva a las mujeres y combatir la impunidad de esta clase de violencias.

En pocos años la institucionalidad responsable, los organismos internacionales, así como la sociedad civil organizada han marcado verdaderos hitos en relación con la defensa de los derechos humanos de las mujeres en los entornos tecnológicos y digitales, pero el Derecho internacional de los derechos humanos no ha abordado aún la enorme cantidad de aristas que la VCMFT implica. Un ejemplo de este vacío es que, a día de hoy, no se han fijado estándares internacionales desde el punto de vista de la protección internacional: el carácter transfronterizo y multijurisdiccional de esta modalidad de violencia trasciende la estatalidad de la protección internacional y exige un cambio de paradigma en relación con el concepto de la nacionalidad de los agentes perseguidores y de los de protección de las víctimas y sobrevivientes, entre otros aspectos, para así ofrecer una protección efectiva a las mujeres perseguidas.

Ante el inabarcable objetivo de acometer el análisis de la situación actual de la VCMFT, este documento sistematiza los principales estándares internacionales –hasta mayo de 2024– sobre la prevención, sanción y erradicación de esta modalidad de violencia, así como los relacionados con la protección de las mujeres establecidos por los sistemas universal, interamericano, europeo y africano, además de por el Derecho comparado; normativa internacional relacionada con los derechos humanos de las mujeres y con el cibercrimen; legislación de diferentes países –especialmente latinoamericanos–[6] en relación con las diferentes tipificaciones de la VCMFT, resoluciones, recomendaciones, observaciones e informes elaborados por organismos internacionales de los ámbitos global y regional y, finalmente, también contiene cuatro relevantes sentencias del Tribunal Europeo de Derechos Humanos, que constituyen una importante fuente de estándares jurisprudenciales en el ámbito del Derecho internacional de los derechos humanos.

A pesar del importante trabajo desarrollado en los últimos años, la prevención, sanción y erradicación de la violencia en línea contra las mujeres está en un estadio aún muy incipiente. Falta mucho por avanzar y en muchas direcciones, pero también son múltiples los esfuerzos en innumerables países, con el apoyo de los organismos internacionales, para abordar esta nueva amenaza a los derechos de las mujeres. Este documento, de hecho, es fruto de ese esfuerzo para aportar al dialogo internacional y transcontinental. Es una herramienta de partida para continuar y provocar con el necesario debate e intercambio de saberes sobre la VCMFT con el objetivo de contribuir al desarrollo de normativas internacionales y nacionales que garanticen el derecho de las mujeres a una vida libre de violencia, de todas las violencias.

6 Este documento tiene un carácter bifronte: de un lado pone en valor algunos de los más relevantes avances en materia de lucha contra la VCMFT; mientras del otro informa, a la vez que nutre, el anteproyecto de la futura Ley Modelo Integral para prevenir, sancionar y erradicar la violencia de género contra las mujeres facilitada por las tecnologías, en curso de elaboración por el MESECVI –CIM- OEA y que cuenta con el apoyo de múltiples organismos internacionales, entre ellos el Programa EUROsociAL.

1. Terminología y definiciones

TERMINOLOGÍA

Organización de Estados Americanos (OEA), Comisión Interamericana de Mujeres (CIM), Mecanismo de Seguimiento de la Convención interamericana para prevenir, sancionar y erradicar la violencia contra la mujer (MESECVI) y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará", de 2022

A la fecha existen a nivel internacional o regional algunos conceptos sobre la violencia de género en contra las mujeres y las niñas cometida a través de las nuevas tecnologías de la información y comunicación (en adelante, "TIC"), si bien sigue siendo una tarea pendiente diseñar una terminología acordada, precisa y estandarizada que abarque la gran variedad de agresiones basadas en el género que las mujeres y las niñas enfrentan cuando acceden al internet.

A través de un análisis de la literatura existente en la materia, se pudo identificar el uso de una amplia gama de conceptos, términos y tipologías acuñadas por agencias internacionales, academia, organizaciones de la sociedad civil, medios de comunicación y plataformas de internet que, si bien identifican rasgos comunes del fenómeno de la violencia en línea, han propiciado, en algunos casos, una confusión alrededor de este fenómeno8.

Esta falta de directrices ha dado lugar a la utilización de términos inapropiados para referirse a los actos que afectan a las mujeres y niñas en línea, tal y como lo comprueba el uso extendido del término 'pornovenganza' para referirse erróneamente a la distribución en línea de material audiovisual de naturaleza íntima o sexual sin consentimiento de la víctima. (Pág. 10)

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, Informe de 18 de junio de 2018

15. La terminología en este ámbito todavía está evolucionando y no es unívoca. En varios documentos oficiales de las Naciones Unidas, en particular la Agenda 2030 para el Desarrollo Sostenible, se hace referencia al término general e inclusivo "tecnología de la información y las comunicaciones" (o TIC), mientras que en otros informes se utilizan los términos "violencia en línea", "violencia digital" o "ciberviolencia". En el presente informe, la Relatora Especial se refiere a "la violencia contra la mujer facilitada por las TIC" como el término más inclusivo, pero utiliza principalmente el término "violencia en línea contra la mujer" como expresión más fácil de usar. Cuando procede, utiliza ambos términos, así como los términos "ciberviolencia" y "violencia facilitada por la tecnología" como alternativas. [...]

Plataforma de Mecanismos de Expertos Independientes sobre la Discriminación y la Violencia contra la Mujer (EDVAW), Informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022

[...] De hecho, la terminología cambia en parte debido a la continua evolución de las TIC y las tecnologías basadas en Inteligencia Artificial, lo que da lugar a una variedad cada vez mayor de formas en que se ejerce dicha violencia. Se debe considerar cuidadosamente la elección de la terminología a fin de evitar términos que sensacionalicen tal violencia o culpen a la víctima. Asimismo, este enfoque puede ayudar a las mujeres y a las niñas a nombrar mejor sus experiencias.

TERMINOLOGÍA

Grupo de Expertos en la Lucha contra la Violencia contra la Mujer y la Violencia Doméstica (GREVIO), Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

24. El término "dimensión digital de la violencia contra las mujeres" se emplea para enfatizar el hecho de que este comportamiento dañino afecta desproporcionadamente a mujeres y niñas y constituye un elemento central de sus experiencias de violencia de género contra las mujeres. Es una violencia perpetrada contra mujeres y niñas que tiene sus raíces en el mismo contexto de desigualdad de las mujeres y del sentido de derecho de los hombres que la violencia psicológica, sexual y física que experimentan las mujeres y las niñas en el mundo fuera de línea.

28. Hasta la fecha, no existe una tipología o definición universal de comportamientos o acciones que se considere que agrupen todas las formas de violencia contra las mujeres perpetradas en línea o mediante tecnología. En cambio, los discursos y enfoques sobre el comportamiento abusivo en línea y los daños perpetrados a través de la tecnología están marcados por términos que se usan indistintamente o de manera inexacta, creando una fragmentación que se ve reforzada por la diversidad de objetivos y perspectivas de los diferentes actores que actualmente están dando forma a la narrativa. Muchos términos que se utilizan actualmente no cubren toda la gama de comportamientos ni resaltan el patrón de género en el abuso. Si bien describen algunas formas muy relevantes de violencia contra las mujeres perpetradas en espacios digitales, no cubren todas las actividades realizadas en línea o mediante tecnología que dañan a mujeres y niñas.

29. GREVIO considera que el término "violencia contra las mujeres en su dimensión digital" o "la dimensión digital de la violencia contra las mujeres" es lo suficientemente amplio como para abarcar tanto los actos de violencia en línea como los perpetrados a través de la tecnología, incluida la tecnología aún por desarrollar. También permite reconocer que no todos los actos de violencia contra las mujeres en la esfera digital son de la misma gravedad, ni todos alcanzan el umbral para el procesamiento penal dentro de cada estado. En vista de la naturaleza cambiante de la tecnología y las oportunidades para comportamientos dañinos, el término "violencia contra las mujeres en su dimensión digital" permitirá que tipos de comportamiento y acciones aún por surgir entren dentro de su competencia. [...]

VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

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, Informe de 18 de junio de 2018

23. [L]a definición de violencia en línea contra la mujer se aplica a todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC [Tecnologías de Información y Comunicación], o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada.

OEA, CIM, MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará", de 2022

Cualquier acción o conducta en contra de la mujer, basada en su género, que le cause muerte, daño o sufrimiento físico, sexual o psicológico, económico o simbólico, en cualquier ámbito de su vida, la cual es cometida, instigada o agravada, en parte o en su totalidad, con la asistencia de las tecnologías de la información y comunicación. (Pág. 12)

[L]a violencia en línea es una manifestación de las relaciones de poder históricamente desiguales entre géneros y uno de los mecanismos sociales mediante los cuales se obliga a las mujeres a permanecer en una situación de subordinación con respecto del hombre, impidiéndoles total o parcialmente el goce de sus derechos humanos y libertades fundamentales y su participación en el desarrollo, el cual ahora está facilitado por la tecnología digital. (Pág. 15)

Consejo de Europa, Comité de la Convención sobre Delitos Cibernéticos, Grupo de Trabajo sobre ciberacoso y otras formas de violencia en línea, especialmente contra mujeres y niños, "Estudio de mapeo sobre ciberviolencia", de 9 de julio de 2018

La ciberviolencia es el uso de sistemas informáticos para causar, facilitar o amenazar con violencia contra individuos que resulte, o pueda resultar, en daño o sufrimiento físico, sexual, psicológico o económico y puede incluir la explotación de las circunstancias, características o vulnerabilidades. (Pág. 5)

Ley de acceso de las mujeres a una vida libre de violencia (México), de 1 de junio de 2021

Artículo 20 quáter.

Violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona entenderá por Tecnologías de la Información y la Comunicación aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos. La violencia digital será sancionada en la forma y términos que establezca el Código Penal Federal.

VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

Ley Nº 5777 de protección integral a las mujeres contra toda forma de violencia (Paraguay)

Artículo 6.l).

Violencia telemática. Es la acción por medio de la cual se difunden o publican mensajes, fotografías, audios, videos u otros que afecten la dignidad o intimidad de las mujeres a través de las actuales tecnologías de información y comunicación, incluido el uso de estos medios para promover la cosificación, sumisión o explotación de la mujer. Se entenderá por "cosificación" a la acción de reducir a la mujer a la condición de cosa.

Plataforma EDVAW, Informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022

La dimensión digital de la violencia contra la mujer comprende cualquier acto de violencia de género contra la mujer que sea cometido, asistido o agravado en parte o en su totalidad por el uso de las tecnologías de la información y la comunicación (TIC), como teléfonos móviles y teléfonos inteligentes, Internet, plataformas de redes sociales o correo electrónico, dispositivos de seguimiento de geolocalización, drones y dispositivos de grabación no conectados a Internet e Inteligencia Artificial (IA), contra una mujer por ser mujer, o afecta a las mujeres de manera desproporcionada. (Pág. 8)

Ley 27736, de modificaciones de la Ley 26485 (Ley Olimpia-Argentina), de 23 de octubre de 2023

Artículo 4.

[...]

i) Violencia digital o telemática: toda conducta, acción u omisión en contra de las mujeres basada en su género que sea cometida, instigada o agravada, en parte o en su totalidad, con la asistencia, utilización y/o apropiación de las tecnologías de la información y la comunicación, con el objeto de causar daños físicos, psicológicos, económicos, sexuales o morales tanto en el ámbito privado como en el público a ellas o su grupo familiar.

En especial conductas que atenten contra su integridad, dignidad, identidad, reputación, libertad, y contra el acceso, permanencia y desenvolvimiento en el espacio digital o que impliquen la obtención, reproducción y difusión, sin consentimiento de material digital real o editado, intimo o de desnudez, que se le atribuya a las mujeres, o la reproducción en el espacio digital de discursos de odio integridad sexual de las mujeres a través de las tecnologías de la información y la comunicación, o cualquier ciberataque que pueda surgir a futuro y que afecte los derechos protegidos en la presente ley.

VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

33. La dimensión digital de la violencia contra las mujeres abarca una amplia gama de comportamientos que entran dentro de la definición de violencia contra las mujeres establecida en el artículo 3.a del Convenio de Estambul. Esta definición comprende "todos los actos de violencia de género contra las mujeres que tengan o puedan tener como resultado daños o sufrimientos físicos, sexuales, psicológicos o económicos para las mujeres, incluidas las amenazas de tales actos, la coerción o la privación arbitraria de la libertad, ya sea que ocurran en la vida pública o privada". Compartir imágenes o vídeos sin consentimiento, coerción y amenazas, incluidas amenazas de violación, acoso sexual y otras formas de intimidación, acoso sexual en línea, suplantación de identidad, acoso en línea o a través del Internet de las cosas, así como abuso psicológico y daño económico perpetrados a través de medios digitales. Los medios contra mujeres y niñas entran todos bajo la definición anterior.

CONTINUUM DE VIOLENCIA EN LÍNEA

OEA, CIM, MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará", de 2022

[La violencia en línea es] parte de un ***continuum*** de violencia contra mujeres y niñas que ahora fluye en el nuevo escenario ***online-offline***. Dada la interrelación de las tecnologías en nuestras vidas, las violencias de género ahora se han entrelazado y mutado en nuestra realidad continuamente conectada, siendo con frecuencia difícil distinguir entre aquella violencia que afecta a una mujer fuera o dentro del internet. (Pág. 14)

(En el mismo sentido: Plataforma EDVAW, Informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022, pág. 9; 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, Informe de 18 de junio de 2018, párr. 14).

Tribunal Europeo de Derechos Humanos (TEDH), Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

49. La violencia en línea, o ciberviolencia, está estrechamente relacionada con la violencia fuera de línea o «en la vida real» y debe considerarse como otra faceta del complejo fenómeno de la violencia doméstica. [...]

(En el mismo sentido: TEDH, Caso Buturuga vs. Rumanía, Sentencia de 11 de febrero de 2020, párrs. 20 y 74-78).

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

F. Considerando que la violencia contra las mujeres y las niñas en toda su diversidad y la violencia de género presentan formas y manifestaciones diferentes pero no mutuamente excluyentes; que la violencia en línea suele estar interrelacionada con la violencia fuera de línea y ser inseparable de esta porque puede precederla, acompañarla o continuarla; que, por tanto, la ciberviolencia de género debe entenderse como una extensión, en el entorno en línea, de la violencia de género fuera de línea;

(En el mismo sentido: párr. 1).

PRESTADOR DE SERVICIOS INTERMEDIARIOS

Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo de 19 de octubre de 2022 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE

Artículo 3. A efectos del presente Reglamento, se entenderá por: [...]

g) «servicio intermediario»: uno de los siguientes servicios de la sociedad de la información:

un servicio de «mera transmisión», consistente en transmitir, en una red de comunicaciones, información facilitada por el destinatario del servicio o en facilitar acceso a una red de comunicaciones,

un servicio de «memoria caché», consistente en transmitir por una red de comunicaciones información facilitada por el destinatario del servicio, que conlleve el almacenamiento automático, provisional y temporal de esta información, prestado con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio, a petición de estos,

un servicio de «alojamiento de datos», consistente en almacenar datos facilitados por el destinatario del servicio y a petición de este; [...]

Convenio sobre ciberdelincuencia de Budapest,. de 23 de noviembre de 2001

Artículo 1. Definiciones.

[...]

c. Por "proveedor de servicios" se entenderá:

Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y

Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

HERRAMIENTAS TECNOLÓGICAS

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

23. [...] Las herramientas tecnológicas que los abusadores pueden utilizar indebidamente para acechar, acosar, vigilar y controlar a las víctimas incluyen teléfonos inteligentes, cámaras y otros equipos de grabación, sistemas de posicionamiento global (GPS) o navegadores satelitales, otros dispositivos conectados a Internet, como relojes inteligentes, rastreadores de actividad física y dispositivos domésticos inteligentes, así como software como ***spyware*** u otras aplicaciones móviles que puedan facilitar la violencia.

ALFABETIZACIÓN DIGITAL

Comisión Interamericana de Derechos Humanos (CIDH), Relatoría Especial para la Libertad de Expresión, Informe "Estándares para una internet libre, abierta e incluyente", de 15 de marzo de 2017

42. [C]onjunto de destrezas, conocimientos y actitudes que necesita una persona para poder desenvolverse funcionalmente dentro de la sociedad de la información y tiene por objeto el desarrollo de habilidades y conocimiento que es permitan "utilizar la tecnología de manera efectiva, desarrollando nuevas oportunidades sociales y económicas en el marco de su sociedad".

2. Estándares del Derecho internacional de los derechos humanos en relación con la violencia en línea contra las mujeres

2.1 Algunas características de la violencia en línea contra las mujeres.

CARACTER TRANSNACIONAL

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con género: la ciberviolencia

15. Subraya el carácter transnacional de la ciberviolencia de género; destaca que la ciberviolencia de género tiene implicaciones transnacionales adicionales, teniendo en cuenta que el uso de las TIC tiene una dimensión transfronteriza; subraya que sus autores utilizan plataformas en línea o teléfonos móviles conectados o alojados en países distintos de aquellos en los que se encuentran las víctimas de la ciberviolencia de género; destaca que los rápidos avances tecnológicos y la digitalización podrían generar nuevas formas de ciberviolencia de género, lo que puede dar lugar a que los autores no sean considerados responsables, reforzando así la cultura de la impunidad;

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[L]a violencia de género en línea tiene además un carácter multijurisdiccional y transnacional, dado que muchos de los actos de abuso se cometen fuera de la jurisdicción de los Estados. (Pág. 15)

(En el mismo sentido: Comité de Derechos Humanos (CDH), 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018, párr. 3; 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, Informe de 18 de junio de 2018, párr 64).

VICTIMIZACIÓN REITERADA

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 8 de marzo de 2024

(Considerando 51) [...] Algunos delitos regulados por la presente Directiva conllevan un riesgo mayor de victimización reiterada, prolongada o incluso continua. Ese riesgo aparece, en particular, en relación con los delitos que implican hacer accesible mediante TIC material resultante de determinados delitos de ciberviolencia, habida cuenta de la facilidad y rapidez con que dicho material puede distribuirse a gran escala y de las dificultades que a menudo existen para retirarlo. Ese riesgo suele persistir incluso después de que se haya dictado una condena. Por consiguiente, a fin de salvaguardar eficazmente los derechos de las víctimas de esos delitos, los Estados miembros deben adoptar las medidas adecuadas con el fin de eliminar de inmediato el material en cuestión. Teniendo en cuenta que la eliminación en origen puede no ser siempre factible, por ejemplo debido a dificultades jurídicas o prácticas relacionadas con la ejecución o el cumplimiento de una orden de eliminación, los Estados miembros deben estar autorizados también para establecer medidas que permitan inhabilitar de inmediato el acceso a dicho material.

ESTEREOTIPOS Y PREJUICIOS DE GÉNERO EN EL ÁMBITO DE LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

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, Informe de 18 de junio de 2018

25. [...] Las mujeres afectadas por la violencia en línea a menudo son objeto de una victimización ulterior debido a estereotipos de género perjudiciales y negativos, prohibidos por el derecho internacional de los derechos humanos. [...]

OEA, CIM, MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará", de 2022

La ciberviolencia en contra de las mujeres y las niñas tiene su origen y es consecuencia de la creación y normalización de estereotipos de género, los cuales están vigentes y se multiplican en espacios e interacciones digitales. [...]

Es importante recordar que las distintas manifestaciones de violencia de género que forman parte de este ***continuum*** poseen un elemento común: todas ellas son formas de coerción, abuso y/o agresión ejercidas con el fin de controlar, limitar o constreñir las vidas, cuerpos, movimientos, condiciones y oportunidades de las mujeres y las niñas, y para mantener, reproducir y perpetuar -en línea y fuera de línea- un sistema de desigualdad y estructuras patriarcales de coerción en el que las mujeres y las niñas se ubican en una posición subordinada frente a los hombres con base en estereotipos nocivos de género.

(En el mismo sentido: MESECVI, Guía para la Aplicación de la Convención de Belém do Pará, pág. 23).

CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018

[L]a violencia contra las mujeres y las niñas, incluso en los contextos digitales, es un fenómeno mundial que hunde sus raíces en la desigualdad histórica y estructural que ha caracterizado las relaciones de poder entre la mujer y el hombre, que refuerza aún más los estereotipos de género y los obstáculos que impiden a las mujeres y las niñas disfrutar plenamente de sus derechos humanos, y que todas las formas de violencia contra las mujeres y las niñas limitan seriamente su participación plena, igualitaria y efectiva en la sociedad, la economía y la toma de decisiones políticas y personales, así como en puestos de liderazgo, y menoscaban su ejercicio y disfrute de los derechos humanos y las libertades fundamentales.

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

36. Recuerda que los estereotipos y las normas de género constituyen el núcleo de la discriminación de género; subraya los efectos sobre la igualdad de género de la reproducción de estereotipos de género en los medios de comunicación y en la publicidad; pide a las empresas y medios de comunicación que refuercen los mecanismos de autorregulación y los códigos de conducta para condenar y combatir los contenidos y la publicidad sexistas, tales como las imágenes y el lenguaje sexistas, las prácticas sexistas y los estereotipos de género;

GRUPOS DE MUJERES QUE ENFRENTAN UN RIESGO MÁS ALTO DE SER VÍCTIMAS DE VIOLENCIA DE GÉNERO EN LÍNEAL

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

H. Considerando que las mujeres jóvenes y las niñas se encuentran en mayor riesgo de sufrir ciberviolencia, en particular ciberacoso y al ciberintimidación; que al menos el 12,5 % de los casos de acoso escolar se producen en línea; que actualmente los jóvenes se conectan a las redes sociales a una edad cada vez más temprana; que estas formas de violencia refuerzan el peso de las desigualdades sociales, ya que las víctimas suelen ser los jóvenes más desfavorecidos; que, según UNICEF, las chicas sufren el doble de acoso que los chicos; que, según esta encuesta, las mujeres son más escépticas en cuanto al uso responsable de sus datos por parte de las empresas tecnológicas; [...]

AC. [...] que algunas mujeres y personas LGBTIQ —feministas, activistas LGBTIQ, artistas, políticos, mujeres en cargos públicos, periodistas, blogueros, defensores de los derechos humanos y otras figuras públicas— se ven particularmente afectadas por la ciberviolencia de género y que ello no solo les causa daños a su reputación y daños y sufrimientos psicológicos, sino que también puede alterar las condiciones de vida de las víctimas y puede dar lugar a invasiones de su privacidad y daños a sus relaciones personales y a su vida familiar y disuadirlas de participar digitalmente en la vida política, social y cultural;

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

(Considerando 17) [...] La ciberviolencia se dirige y afecta especialmente a las mujeres políticas, periodistas y defensoras de los derechos humanos. Los defensores de los derechos humanos son personas, grupos u organizaciones que promueven y protegen los derechos humanos y las libertades fundamentales universalmente reconocidos. La ciberviolencia puede tener el efecto de silenciar a las mujeres y obstaculizar su participación social en pie de igualdad con los hombres. La ciberviolencia afecta también de manera desproporcionada a las mujeres y las niñas en los entornos educativos, como escuelas y universidades, con consecuencias perjudiciales para la continuación de su educación y para su salud mental, causa exclusión social, ansiedad y tendencia a la autolesión, y, en casos extremos, puede llevar al suicidio.

(En el mismo sentido: OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará", de 2022, págs. 20-21).

2.2 Contexto material actual en relación con la violencia en línea contra las mujeres

LA MAGNITUD DE LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

Plataforma EDVAW, Informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022

La dimensión digital de la violencia contra la mujer es alarmantemente frecuente. Según un estudio de 2015 realizado por la Comisión de Banda Ancha para el Desarrollo Sostenible de las Naciones Unidas, casi tres cuartas partes de las mujeres han experimentado algún tipo de violencia de género en línea, y casi dos tercios de los autores son hombres (Comisión de Banda Ancha para el Desarrollo Sostenible de las Naciones Unidas, 2015). En 2020, un estudio de la Economist Intelligence Unit que abarcó 45 países reveló que el 85 % de las mujeres ha experimentado o presenciado violencia en línea y facilitada por la tecnología, desde el 74 % en Europa, el 91 % en América Latina y el Caribe y el 90 % en África (Economist Intelligence Unit, 2021). Amnistía Internacional publicó un estudio comparativo realizado en Europa, Estados Unidos y Nueva Zelanda que puso de manifiesto que casi una cuarta parte de las mujeres entrevistadas habían experimentado violencia de género en línea y facilitada por la tecnología al menos una vez en su vida (Amnistía Internacional, 2017).

En 2021, ONU Mujeres publicó un informe sobre Oriente Medio en el que se reveló que el 60 % de las mujeres habían sufrido violencia en línea y facilitada por la tecnología y la habían denunciado en el último año (ONU Mujeres, 2021b). En 2020, Pollicy, un colectivo feminista ubicado en Uganda, realizó una encuesta sobre la violencia en línea contra la mujer en Etiopía, Kenia, Sudáfrica, Senegal y Uganda que encontró que el 28 % de las mujeres había sufrido diversas formas de violencia en línea y facilitada por la tecnología (Pollicy, 2021). Un estudio nacional encargado por el Parlamento brasileño en 2018 encontró que 2 788 de los 68 000 casos penales de violencia contra la mujer tenían una dimensión digital, siendo la mayor parte de los delincuentes parejas actuales o anteriores (ONU Mujeres y OEA/CIM/MESECVI, 2022).

LAS TIC COMO FACILITADORAS DE NUEVAS FORMAS DE VIOLENCIA Y AMPLIFICADORAS Y REPRODUCTORAS DE LAS YA EXISTENTES

Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", de 24 de junio de 2020

15. [E]l uso de las TIC también ha permitido un discurso de odio y un discurso peligroso en contra de ciertos grupos raciales y religiosos, así como la discriminación, las agresiones y la violencia por motivos de género, en particular la violencia contra las mujeres y las niñas. Esta situación suele reflejar y puede exacerbar una serie de estereotipos raciales y de género nocivos, la discriminación y la violencia fuera de la Red. La violencia en la Red contra ciertas minorías raciales y religiosas y contra las mujeres y las niñas ha experimentado un brusco aumento en los últimos años y puede conllevar una limitación de la participación de las mujeres en las plataformas digitales. Esta conclusión es especialmente manifiesta cuando son activistas de derechos civiles e igualdad racial y grupos de mujeres y niñas los que organizan las reuniones. Los actos de violencia y maltrato en la Red contra minorías raciales y religiosas y contra las mujeres y las niñas provoca que muchos se practiquen la autocensura o limiten sus interacciones en línea, lo que supone una restricción del ejercicio de sus derechos, en particular el derecho a la libertad de reunión pacífica. Las singularidades raciales y de género y las posibilidades que brindan las TIC para intimidar, amenazar y lesionar a las mujeres y las niñas, incluso fuera de la Red, exigen una reflexión cuidadosa y profunda, así como medidas específicas de reacción.

(En el mismo sentido: GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, párr. 30).

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

23. [...] Las formas de violencia contra las mujeres en línea y facilitadas por Internet se han vuelto cada vez más comunes, en particular con el uso de plataformas de redes sociales y otras aplicaciones técnicas [...].

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, Informe de 18 de junio de 2018

12. Las formas de violencia en línea contra la mujer y facilitadas por las TIC se han vuelto cada vez más comunes, sobre todo con la utilización, cotidiana y generalizada, de las plataformas de medios sociales y otras aplicaciones técnicas. [...]

14. [...] A pesar de las ventajas y el potencial de empoderamiento de Internet y de las TIC, las mujeres y las niñas de todo el mundo han expresado en forma creciente su preocupación por el contenido y el comportamiento dañinos, sexistas, misóginos y violentos en línea. Por lo tanto, es importante reconocer que Internet se está utilizando en un entorno más amplio de discriminación y violencia por razón de género, generalizado, estructural y sistémico contra las mujeres y las niñas, que determina su acceso a Internet y otras TIC y su uso de estas. Las nuevas formas de TIC han facilitado nuevos tipos de violencia por razón de género y desigualdad de género en el acceso a las tecnologías, que impiden a la mujeres y las niñas el pleno disfrute de sus derechos humanos y de su capacidad para lograr la igualdad de género.

LAS TIC COMO FACILITADORAS DE NUEVAS FORMAS DE VIOLENCIA Y AMPLIFICADORAS Y REPRODUCTORAS DE LAS YA EXISTENTES

20. Debido a la facilidad de acceso y la divulgación de contenidos en el entorno digital, las estructuras sociales, económicas, culturales y políticas, así como las formas conexas de discriminación por motivos de género y los modelos patriarcales que dan lugar a la violencia de género en general se reproducen, y a veces se amplifican y redefinen en las TIC, al tiempo que surgen nuevas formas de violencia. [...]

30. [...] Todas las formas de violencia de género en línea se utilizan para controlar y atacar a las mujeres y mantener y reforzar las normas, los papeles y las estructuras patriarcales, y una relación de poder desigual. [...]

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

(Considerando 18) El uso de las TIC conlleva un riesgo de amplificación fácil, rápida y generalizada de determinadas formas de ciberviolencia, con el claro riesgo de crear o intensificar daños profundos y duraderos en la víctima. El potencial de amplificación, que es un requisito previo para la comisión de varios delitos de ciberviolencia definidos en la presente Directiva, debe reflejarse en el elemento de "accesible al público" de determinado material mediante TIC. Los términos "accesible al público" y "accesible públicamente" deben entenderse en referencia a la posibilidad de llegar a un número de personas. Esos términos deben interpretarse y aplicarse teniendo en cuenta las circunstancias pertinentes, incluidas las tecnologías utilizadas para hacer accesible ese material. [...]

(Considerando 22) El incremento del uso de internet y de las redes sociales ha dado lugar a un marcado aumento de la incitación pública a la violencia y al odio, también por motivos de sexo o género, en los últimos años. La fácil, rápida y amplia difusión de los discursos de odio a través del mundo digital se ve potenciada por el efecto de desinhibición en línea, ya que el supuesto anonimato en internet y el sentimiento de impunidad reducen la inhibición de la gente a proferir tales discursos. Las mujeres son a menudo blanco de odio sexista y misógino en línea, que puede intensificarse hasta convertirse en delito de odio fuera de línea. Esto debe interceptarse en una fase temprana. El lenguaje utilizado en este tipo de incitación no siempre hace referencia directa al sexo o al género de la persona o personas atacadas, pero los prejuicios que la motivan pueden deducirse del contenido general o el contexto de la incitación.

LOS DIFERENTES TIPOS DE VIOLENCIA EN LÍNEA

Plataforma EDVAW, Informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022

[S]urgen cuatro tipos o categorías principales de violencia en línea y facilitada por la tecnología: en primer lugar, formas de acoso, violencia o abuso que son facilitadas por tecnologías específicas y dispositivos habilitados por la tecnología, como la violencia de pareja íntima llevada a cabo a través del uso de tecnologías que utilizan programas espías y otros dispositivos de seguimiento; en segundo lugar, el abuso que tiene lugar y se amplifica en línea, como formas de abuso sexual basado en imágenes tales como el intercambio no consentido de imágenes íntimas; en tercer lugar, cuando la tecnología ha generado una nueva forma de abuso, como la pornografía falsa y el abuso de nuestra identidad digital en el metaverso; y, en cuarto lugar, cuando el entorno en línea se utiliza para permitir que se produzcan violencia y abuso, como el uso de las redes sociales como elemento central de diversas formas de violencia sexual contra las mujeres y las niñas.

La violencia contra las mujeres en línea y facilitada por la tecnología abarca por lo tanto una amplia gama de conductas, como todas las formas de abuso sexual basado en imágenes (por ejemplo, la creación, difusión, distribución o intercambio en línea de fotografías, vídeos o clips de audio de naturaleza sexual o íntima sin el consentimiento de la víctima), así como la "pornografía falsa" generada por IA; el acceso, la manipulación o la distribución no autorizados de datos personales (por ejemplo, el doxeo); el robo de identidad o la suplantación de identidad (por ejemplo, la creación de perfiles falsos); actos que dañan la reputación o la credibilidad de una persona; actos que impliquen vigilancia y seguimiento de una persona (por ejemplo, acecho en línea); el acoso (sexual) en línea; el ciberacoso; las amenazas y los abusos sexuales y físicos en línea; y el acoso y el abuso de identidades digitales como los avatares. (Pág. 8)

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

23. [...] La violencia en línea contra las mujeres puede manifestarse de diferentes formas y a través de diferentes medios, como el acceso, uso, manipulación, difusión o intercambio no consensuado de datos, fotografías o videos privados, incluidas imágenes sexualizadas [...].

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, Informe de 18 de junio de 2018

30. [...] La tecnología ha transformado muchas formas de violencia de género en algo que puede cometerse a distancia, sin contacto físico y que va más allá de las fronteras mediante el uso de perfiles anónimos para intensificar el daño a las víctimas. [...]

31. Las TIC pueden utilizarse directamente como medios para hacer amenazas digitales e incitar a la violencia de género, así como amenazas de violencia física y/o sexual, violación, asesinato, comunicaciones en línea no deseadas y que constituyen acoso, o incluso alentar a otros a infligir daños físicos a mujeres. También pueden entrañar la difusión de mentiras que perjudican la reputación, sabotaje electrónico en forma de correo basura y virus malignos, suplantación de la identidad de la víctima en línea y envío de mensajes de correo electrónico o correo basura insultantes, blogs, tuits u otras comunicaciones en línea en nombre de la víctima. La violencia contra la mujer facilitada por las TIC también pueden cometerse en el lugar de trabajo o

LOS DIFERENTES TIPOS DE VIOLENCIA EN LÍNEA

mediante los denominados actos de violencia "por motivos de honor" o de violencia doméstica cometidos por parejas íntimas. [...]

32. Las herramientas de las TIC también se utilizan para la trata de mujeres y niñas, o como una amenaza para obligarlas a aceptar situaciones de trata. Los autores de estos abusos pueden amenazar con revelar información privada en Internet para mantener el poder y el control sobre sus víctimas e impedirles que se liberen y/o denuncien el abuso y defiendan sus derechos ante los tribunales.

[...]

34. La violencia en línea contra la mujer puede manifestarse en diversas formas y por diferentes medios, como el acceso, la utilización, la manipulación, la difusión o el intercambio de datos, información y/o contenidos, fotografías o vídeos privados no consentidos, incluidas imágenes sexualizadas, audioclips y/o vídeoclips o imágenes editadas con Photoshop.

(En el mismo sentido: OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022, págs. 23 y 24; GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, párr. 41).

LOS DAÑOS CAUSADOS A LAS MUJERES POR LA VIOLENCIA EN LÍNEA Y SU ESTRECHA RELACIÓN CON EL GÉNERO

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

23. [...] Todas las formas de violencia de género en línea se utilizan para controlar y atacar a las mujeres y para mantener y reforzar las normas, roles y estructuras patriarcales y una relación de poder desigual [...].

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, Informe de 18 de junio de 2018

25. Las consecuencias y los daños causados por las diferentes manifestaciones de violencia en línea guardan una estrecha relación con el género, habida cuenta de que las mujeres y las niñas sufren un estigma particular en el contexto de la desigualdad estructural, la discriminación y el patriarcado. Las mujeres afectadas por la violencia en línea a menudo son objeto de una victimización ulterior debido a estereotipos de género perjudiciales y negativos, prohibidos por el derecho internacional de los derechos humanos. [...]

42. [...] Los datos y estudios pertinentes han demostrado que, en la mayoría de los casos, la violencia en línea no es un delito neutro en cuanto al género. Los estudios sobre la dimensión de género de la violencia en línea indican efectivamente que el 90% de las víctimas de la distribución digital no consensuada de imágenes íntimas son mujeres.

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

28. Señala que la ciberviolencia de género puede tener un gran impacto con consecuencias graves y para toda la vida para las víctimas, como efectos fisiológicos y sobre la salud mental, incluidos el estrés, los problemas de concentración, la ansiedad, los ataques de pánico, la baja autoestima, la depresión, el trastorno por estrés postraumático, el aislamiento social, la falta de confianza y de sentimiento de control, el miedo, la autolesión y la ideación suicida;

29. Señala que el impacto de la ciberviolencia de género en las víctimas puede provocar daños a la reputación, problemas físicos y médicos, perturbaciones en la vida de la víctima, violaciones del derecho a la intimidad y retirada de entornos en línea y fuera de línea; [...]

(En el mismo sentido: Plataforma EDVAW, Informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022, pág. 9; OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022, pág. 132; GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, párr. 20)

VIOLENCIA EN LÍNEA E INTERSECCIONALIDAD

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

Tal y como sucede con la violencia de género fuera de internet, la violencia en línea es interseccional y se incrementa de acuerdo a indicadores de identidad como la raza, etnia, estrato socioeconómico, orientación sexual o nacionalidad. Según lo ha referido el CEVI, "la convergencia de múltiples formas de discriminación aumenta el riesgo de que algunas mujeres sean víctimas de discriminación específica, compuesta o estructural", lo cual es evidente en el ciberespacio en donde la violencia de género se está ejerciendo con la intención de disciplinar, controlar y/o silenciar a mujeres que se definen de formas múltiples. (Pág. 20)

LAS CONSECUENCIAS DE LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

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, Informe de 18 de junio de 2018

26. Los actos de violencia en línea pueden llevar a las mujeres a abstenerse de usar Internet. Las investigaciones indican que el 28% de las mujeres que fueron objeto de violencia basada en las TIC han reducido deliberadamente su presencia en línea. Otras consecuencias comunes son el aislamiento social, que lleva a las víctimas o supervivientes a retirarse de la vida pública, incluidos la familia y los amigos, y la movilidad limitada, es decir, la pérdida de libertad para desplazarse en condiciones de seguridad.

(En el mismo sentido: OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022, pág. 95).

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

AD. Considerando que la ciberviolencia de género suele dar lugar a la autocensura y que esa situación puede tener un impacto perjudicial en la vida profesional y en la reputación de las víctimas de la ciberviolencia de género; que las amenazas violentas y por motivos de género provocan que, a menudo, las víctimas recurran al uso de pseudónimos, adopten un comportamiento discreto en línea, decidan suspender, desactivar o eliminar permanentemente sus cuentas en línea o incluso abandonen por completo su profesión; que esto puede silenciar las voces y opiniones de las mujeres y agravar la desigualdad de género ya presente en la vida política, social y cultural; que el aumento de la ciberviolencia de género a la que se enfrentan las mujeres puede impedirles participar en mayor medida en el propio sector digital, lo que consolida una concepción, un desarrollo y una aplicación de las nuevas tecnologías marcados por el género y provoca la reproducción de las prácticas y estereotipos discriminatorios existentes que contribuyen a normalizar la ciberviolencia de género;

LOS DIFERENTES TIPOS DE DAÑO QUE PUEDE CAUSAR LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

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, de 18 de junio de 2018

27. Los actos de violencia por razón de género contra las mujeres y las niñas en línea y facilitados por las TIC incluyen las amenazas de dichos actos que dan lugar, o podrían dar lugar, a daños o sufrimientos psicológicos, físicos, sexuales o económicos a las mujeres. Pueden causar un alto grado de daño psicológico debido a la magnitud y la recurrencia de esos actos. Las víctimas y las supervivientes experimentan depresión, ansiedad y miedo y, en algunos casos, hasta tendencias suicidas. La violencia facilitada por la tecnología también puede dar lugar a daños físicos (incluidos suicidios), así como perjuicios económicos. [...] El riesgo de daños se deriva de los contenidos (imágenes sexistas, misóginas, degradantes y estereotipadas de la mujer, pornografía en línea) y los comportamientos en línea (acoso moral, hostigamiento criminal o intimidación facilitados y perpetrados a través de medios sociales, aplicaciones para el rastreo y tecnología para la elaboración de perfiles criminológicos).

OEA, CIM, MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará", de 2022

A la fecha persiste una falta de estudios sobre la naturaleza, características y prevalencia de los daños mediados por la tecnología que viven las mujeres y niñas individual y colectivamente. A pesar de la creciente digitalización y la cada vez más estrecha interrelación entre la vida ***online*** y ***offline***, en general, hay una falta de reconocimiento sobre la seriedad de los daños que conlleva la violencia digital de género, los cuales son usualmente considerados como 'no reales' bajo la excusa de su 'virtualidad'.

[...]

[L]os daños por conductas en línea no difieren en su impacto de los daños ocasionados por la violencia fuera de línea, afectando a las víctimas de forma real e inminente a corto y largo plazo en todos los niveles de su desarrollo individual, vida privada y relaciones sociales. La violencia en línea en contra de las mujeres y las niñas puede afectar de forma desproporcionada su identidad, crecimiento y desarrollo personal, dignidad, libertad y privacidad, generar daños en su integridad física y emocional, daños sexuales y económicos, además de impactar en su confianza y limitar el control sobre sus propias vidas y su habilidad para alcanzar metas profesionales. (Pág. 23).

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

43. Todas las formas de violencia contra las mujeres perpetradas en la esfera digital tienen un impacto psicológico y podrían clasificarse como violencia psicológica ejercida en línea y con el uso de tecnología. [...] Además, las formas de violencia psicológica ejercidas en el contexto de la violencia doméstica adquieren formas radicales cuando se combinan con las nuevas tecnologías. [...]

46. La violencia psicológica en línea también puede adoptar la forma de intimidación, amenazas a las víctimas o sus familiares, insultos, vergüenza y difamación. [...]

LA POSIBILIDAD DE EXTRATERRITORIALIDAD DE LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

47. Otra forma de violencia psicológica es el abuso económico, que se define como el control de la capacidad de una mujer para adquirir, utilizar y mantener recursos económicos. [...]

48. En los foros digitales, el abuso económico puede manifestarse como el control de las cuentas bancarias y las actividades financieras de la víctima a través de la banca por Internet, dañando la calificación crediticia de la víctima mediante el uso de tarjetas de crédito sin permiso o la presentación de todos los contratos financieros (arrendamientos, préstamos, servicios públicos, etc. .) en nombre de la víctima y no realizar los pagos a tiempo o no realizarlos (en particular, pagos de pensión alimenticia).

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

AE. Considerando que la ciberviolencia de género tiene repercusiones directas en la salud y el bienestar sexual, físico y psicológico de las mujeres, así como un impacto social y económico negativo; que la ciberviolencia de género repercute negativamente en la capacidad de las víctimas para ejercer plenamente sus derechos fundamentales, lo que, a su vez, tiene graves consecuencias para la sociedad y la democracia en su conjunto;

AF. Considerando que el impacto económico negativo de la violencia de género y de los problemas de salud mental que provoca puede repercutir gravemente en las víctimas, también en su capacidad para buscar empleo, y puede ser la causa de problemas financieros; que el impacto económico de la violencia de género puede comprender también uno laboral, como una menor presencia en el trabajo o un riesgo de que se vea comprometida la situación laboral, lo que puede provocar la pérdida de puestos de trabajo o una menor productividad; que las repercusiones de la ciberviolencia de género en la salud mental pueden ser complejas y a largo plazo; que las repercusiones en la salud mental de la ciberviolencia de género, como la ansiedad, la depresión y los síntomas postraumáticos continuos, tienen implicaciones interpersonales, sociales, jurídicas, económicas y políticas perjudiciales y, en última instancia, afecta a los medios de subsistencia y a la identidad de la juventud; que algunas de estas repercusiones agravan otras formas de discriminación, exacerbando las formas de discriminación y desigualdad ya existentes;

LA POSIBILIDAD DE EXTRATERRITORIALIDAD DE LA VIOLENCIA EN LÍNEA CONTRA LAS MUJERES

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, Informe de 18 de junio de 2018

64. El hecho de que las violaciones se cometan fuera de los límites territoriales y la jurisdicción de los Estados también dificulta a las autoridades, incluidos los organismos encargados de hacer cumplir la ley, la detección, investigación y enjuiciamiento de los autores y el otorgamiento de reparación a los supervivientes de la violencia por razón de género. Además, puede requerir la cooperación extraterritorial entre Estados.

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[L]a violencia de género en línea tiene además un carácter multijurisdiccional y transnacional, dado que muchos de los actos de abuso se cometen fuera de la jurisdicción de los Estados28. Esta forma de violencia implica además la "utilización y adaptación continuas de las tecnologías digitales por los autores de esos actos para evitar la detección y la investigación", lo cual dificulta a las autoridades su atención, la sanción de los responsables y la reparación de las víctimas. (Pág. 15)

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

23. [...] La tecnología ha transformado muchas formas de violencia de género en algo que puede perpetrarse a distancia, sin contacto físico y más allá de las fronteras. [...]

LA VIOLENCIA EN LÍNEA CONTRA DEFENSORAS DE DERECHOS HUMANOS, PERIODISTAS, MUJERES QUE PARTICIPAN EN LA VIDA POLÍTICA Y OTROS COLECTIVOS

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, Informe de 18 de junio de 2018

29. Las defensoras de los derechos humanos, las periodistas y las mujeres que participan en actividades políticas son objeto de ataques directos, y amenazadas, acosadas y hasta asesinadas por su labor. Reciben amenazas en línea, generalmente de carácter misógino, a menudo de índole sexual y específicamente relacionadas con el género. La naturaleza violenta de estas amenazas a menudo conduce a la autocensura. Algunas de ellas han recurrido al uso de seudónimos, mientras que otras mantienen perfiles bajos en línea, un enfoque que puede tener un efecto perjudicial en su vida profesional y reputación. Otras deciden suspender, desactivar o suprimir sus cuentas en línea en forma permanente, o abandonar la profesión por completo. En última instancia, los abusos en línea contra las mujeres periodistas y las mujeres en los medios de comunicación son un ataque directo a la visibilidad de las mujeres y su participación plena en la vida pública. A su vez, el anonimato de los autores aumenta el temor a la violencia, lo que ha dado lugar a la sensación de inseguridad y angustia de las víctimas. Además de los efectos en las personas, una grave consecuencia de la violencia de género en línea y facilitada por las TIC es una sociedad en que las mujeres ya no se sienten seguras en línea o fuera de línea, debido a la impunidad generalizada de los autores de la violencia de género. La violencia en línea contra la mujer no solo viola el derecho de la mujer a llevar una vida libre de violencia y a participar en línea, sino que también socava el ejercicio democrático y la buena gobernanza y, por lo tanto, crea un déficit democrático.

Unión Parlamentaria, Informe "Sexismo, acoso y violencia contra las mujeres parlamentarias", de 2017

En cinco regiones, el 82 por ciento de las parlamentarias denunció haber experimentado algún tipo de violencia sexual durante su mandato. Esta incluía comentarios, gestos e imágenes de naturaleza sexista o sexualmente humillante, amenazas y acoso laboral. Las mujeres citaban que el canal más habitual por el que sufrían este tipo de violencia eran los medios sociales, y cerca de la mitad (el 44 por ciento) denunciaron haber recibido amenazas de muerte, violación, agresión o secuestro dirigidas contra ellas o sus familias. El 65 por ciento había sido objeto de comentarios sexistas, principalmente por parte de parlamentarios (Pág. 3).

(En el mismo sentido: CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018, pág. 3; OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022, pág. 21; GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, párr. 45)

2.3. Tipos específicos de violencia en línea contra las mujeres

A) Jurisdicción

JURISDICCIÓN

Convenio sobre ciberdelincuencia de Budapest, de 23 de noviembre de 2001

Artículo 22. Jurisdicción.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:

a) En su territorio; o

b) a bordo de un buque que enarbole pabellón de dicha Parte; o

c) a bordo de una aeronave matriculada según las leyes de dicha Parte; o

d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos.

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

Artículo 12. Jurisdicción.

1. Cada Estado miembro adoptará las medidas necesarias para establecer su jurisdicción respecto de los delitos a que se refieren los artículos 3 a 9 cuando:

a) el delito se haya cometido total o parcialmente dentro de su territorio, o

b) el autor del delito sea uno de sus nacionales.

2. Los Estados miembros informarán a la Comisión cuando decidan ampliar su jurisdicción a los delitos a que se refieren los artículos 3 a 9 que hayan sido cometidos fuera de su territorio, cuando:

a) el delito se haya cometido contra uno de sus nacionales o contra un residente habitual en su territorio, o

b) el autor del delito sea residente habitual en su territorio.

JURISDICCIÓN

3. Los Estados miembros garantizarán que la jurisdicción que hayan establecido en relación con los delitos a que se refieren los artículos 5 a 9 incluya las situaciones en las que el delito se cometa mediante TIC a las que se acceda desde su territorio, independientemente de que el prestador de servicios intermediarios esté o no establecido en su territorio.

[...]

5. En los casos a que se refiere el apartado 1, letra b), los Estados miembros adoptarán las medidas necesarias para garantizar que el ejercicio de su jurisdicción no esté supeditado a la condición de que las actuaciones judiciales solo puedan iniciarse a raíz de una denuncia hecha por la víctima en el lugar donde se haya cometido el delito o a raíz de una denuncia del Estado del lugar en el que se haya cometido el delito.

B) Competencia

COMPETENCIA

Convenio sobre ciberdelincuencia de Budapest, de 23 de noviembre de 2001

Artículo 44. Competencia.

1. Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para establecer su competencia con respecto a cualquiera de los delitos previstos en el presente Convenio cuando el delito sea cometido:

a) en su territorio; o
b) a bordo de un buque que enarbole su pabellón; o
c) a bordo de una aeronave matriculada de conformidad con sus leyes internas; o
d) por uno de sus nacionales; o
e) por una persona que tenga su residencia habitual en su territorio.

2. Las Partes se esforzarán por adoptar las medidas legislativas o de otro tipo necesarias para establecer su competencia con respecto a cualquiera de los delitos previstos en el presente Convenio cuando la víctima del delito sea uno de sus nacionales o una persona con residencia habitual en su territorio.

3. A efectos de la persecución de los delitos previstos en los artículos 36, 37, 38 y 39 del presente Convenio, las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que su competencia no esté subordinada a la condición de que los hechos también estén tipificados en el territorio en el que se hayan cometido.

4. A efectos de la persecución de los delitos previstos en los artículos 36, 37, 38 y 39 del presente Convenio, las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que su competencia con respecto a los puntos d y e del apartado 1 no esté subordinada a la condición de que la apertura de diligencias venga precedida de una demanda de la víctima o de una denuncia del Estado del lugar en el que el delito haya sido cometido.

5. Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para establecer su competencia con respecto a cualquiera de los delitos previstos en el presente Convenio en los casos en los que el presunto autor se encuentre presente en su territorio y no pueda ser extraditado a otro Estado Parte únicamente por razón de su nacionalidad.

6. Cuando varias Partes reivindiquen su competencia con respecto a un presunto delito de los previstos en el presente Convenio, las Partes en cuestión se pondrán de acuerdo, en su caso, a efectos de determinar aquella que se encuentre en mejor situación de tramitar las diligencias.

7. Sin perjuicio de las normas generales de derecho internacional, el presente Convenio no excluye ninguna competencia penal ejercida por una Parte de conformidad con su legislación interna.

C) Circunstancias modificativas de la responsabilidad

CIRCUNSTANCIAS AGRAVANTES

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

Artículo 11. Circunstancias agravantes.

En la medida en que las siguientes circunstancias no formen parte de los elementos constitutivos de los delitos a que se refieren los artículos 3 a 8, los Estados miembros adoptarán las medidas necesarias para garantizar que, en relación con los delitos pertinentes a que se refieren dichos artículos, pueda considerarse circunstancia agravante una o más de las siguientes, de conformidad con el Derecho nacional:

a) que el delito, u otro delito de violencia contra las mujeres o de violencia doméstica, se haya cometido reiteradamente;

b) que el delito se haya cometido contra una persona considerada vulnerable por circunstancias particulares, como una situación de dependencia o un estado de discapacidad física, mental, intelectual o sensorial;

c) que el delito se haya cometido contra un menor;

d) que el delito se haya cometido en presencia de un menor;

e) que el delito haya sido cometido por dos o más personas actuando conjuntamente;

f) que el delito haya ido precedido o acompañado de niveles extremos de violencia;

g) que el delito se haya cometido utilizando un arma o amenazando con utilizarla;

h) que el delito se haya cometido utilizando la fuerza o amenazando con utilizarla, o con coacción;

i) que la conducta haya provocado la muerte de la víctima o le haya causado graves lesiones físicas o psicológicas;

j) que el autor haya sido condenado con anterioridad por delitos de la misma naturaleza;

k) que el delito se haya cometido contra un cónyuge o excónyuge o contra una pareja o expareja;

l) que el delito haya sido cometido por un miembro de la familia de la víctima o por una persona que conviva con la víctima;

m) que el delito se haya cometido abusando de una posición reconocida de confianza, autoridad o influencia;

n) que el delito se haya cometido contra alguien por ser esa persona representante público, periodista o defensora de los derechos humanos;

o) que la intención del delito fuera preservar o restaurar el llamado «honor» de una persona, una familia, una comunidad u otro colectivo similar;

p) que la intención del delito fuera castigar a la víctima por su orientación sexual, género, color, religión, origen social o convicciones políticas.

(En el mismo sentido, Convenio del Consejo de Europa sobre prevención y lucha contra las mujeres y la violencia doméstica (Convenio de Estambul), de 2011, artículo 41).

CIRCUNSTANCIAS AGRAVANTES

Código Penal Federal (México)

Artículo 199 decies.

El mínimo y el máximo de la pena [del delito de violación a la intimidad sexual] se aumentará hasta en una mitad:

I) Cuando el delito sea cometido por el cónyuge, concubinario o concubina, o por cualquier persona con la que la víctima tenga o haya tenido una relación sentimental, afectiva o de confianza;

II) Cuando el delito sea cometido por un servidor público en ejercicio de sus funciones;

III) Cuando se cometa contra una persona que no pueda comprender el significado del hecho o no tenga la capacidad para resistirlo;

IV) Cuando se obtenga algún tipo de beneficio no lucrativo;

V) Cuando se haga con fines lucrativos, o

VI) Cuando a consecuencia de los efectos o impactos del delito, la víctima atente contra su integridad o contra su propia vida.

D) Autoría y participación

INDUCCIÓN, TENTATIVA Y COMPLICIDAD

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

Artículo 9. Inducción, complicidad y tentativa.

1. Los Estados miembros garantizarán que sea punible como delito la inducción a la comisión de cualquiera de los delitos a que se refieren los artículos 3 a 6 y el artículo 7, párrafo primero, letra b). [Mutilación genital femenina; matrimonio forzoso; difusión de material íntimo o manipulado; ciberacecho; y ciberacoso en el caso de conductas amenazantes con graves daños psicológicos]

2. Los Estados miembros garantizarán que sea punible como delito la complicidad en la comisión de cualquiera de los delitos a que se refieren el artículo 3, párrafo primero, letra a), y los artículos 4 a 8. [La escisión, la infibulación o cualquier otra mutilación de la totalidad o parte de los labios mayores, los labios menores o el clítoris; matrimonio forzoso; difusión de material íntimo o manipulado; ciberacecho; y ciberacoso] [...]

Convenio sobre ciberdelincuencia de Budapest, de 23 de noviembre de 2001

Artículo 11. Tentativa y complicidad.

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de las delitos previstos de conformidad con los artículos 3 a 5 [interceptación ilícita, interferencia en los datos e interferencia del sistema] 7 [falsificación informática], 8 [fraude informático], 9.1.a) y c) [pornografía infantil] del presente Convenio, cuando dicha tentativa sea intencionada.

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículo.

(En el mismo sentido, Convenio del Consejo de Europa sobre prevención y lucha contra las mujeres y la violencia doméstica (Convenio de Estambul), de 2011, artículo 41).

E) Prescripción

PLAZOS DE PRESCRIPCIÓN

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

Artículo 13. Plazos de prescripción.

1. Los Estados miembros adoptarán las medidas necesarias para establecer un plazo de prescripción que posibilite la investigación, el enjuiciamiento, el juicio oral y la resolución judicial de los delitos a que se refieren los artículos 3 y 9 durante un período de tiempo suficiente a partir de la comisión de dichos delitos, de modo que estos se puedan perseguir de manera eficaz. El plazo de prescripción será proporcional a la gravedad del delito de que se trate.

2. Cuando la víctima sea un menor, el plazo de prescripción de los delitos a que se refiere el artículo 3 empezará a correr, como muy pronto, en el momento en el que la víctima haya cumplido dieciocho años.

F) Tipos de delitos

CIBERACECHO O CIBERVIGILANCIA

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 8 de marzo de 2022

(Considerando 21) El ciberacecho es una forma moderna de violencia que a menudo se comete contra familiares o personas que viven en el mismo hogar que el autor, aunque también lo cometen exparejas o conocidos. Normalmente, el autor hace un uso indebido de la tecnología para intensificar un comportamiento coactivo y controlador, la manipulación y la vigilancia, incrementando con ello el miedo y la ansiedad de la víctima y su aislamiento gradual de amigos y familiares y del trabajo. Por lo tanto, deben establecerse normas mínimas sobre el ciberacecho. El delito de ciberacecho debe comprender la vigilancia reiterada y continua de la víctima sin su consentimiento o sin autorización legal mediante TIC. Esto podría conseguirse mediante el tratamiento de los datos personales de la víctima, por ejemplo a través de una usurpación de identidad, del robo de contraseñas, del pirateo de los dispositivos de la víctima, de la activación furtiva de software que registre las pulsaciones que se realizan en el teclado para así obtener acceso a espacios privados de la víctima, a través de la instalación de aplicaciones de geolocalización, incluidos programas informáticos de acecho (***stalkerware***), o robando dispositivos de la víctima. Además, el delito de ciberacecho debe comprender el seguimiento de las víctimas, sin su consentimiento o autorización, utilizando dispositivos tecnológicos conectados a través de la internet de las cosas, como los electrodomésticos inteligentes. Sin embargo, pueden darse situaciones en las que la vigilancia se realice por motivos legítimos, por ejemplo, en el contexto del seguimiento del paradero y la actividad en línea de los hijos por parte de sus progenitores, del seguimiento de la salud de personas enfermas, mayores, vulnerables o con discapacidad por parte de sus familiares, o del seguimiento de los medios de comunicación y la inteligencia de fuentes abiertas.

Artículo 6. Ciberacecho.

Los Estados miembros garantizarán que sea punible como delito la conducta intencionada de someter reiterada o continuamente a otra persona a vigilancia, sin el consentimiento de esa persona o una autorización legal para hacerlo, mediante TIC, a fin de rastrear u observar los movimientos y actividades de dicha persona, cuando sea probable que tal conducta cause graves daños a esa persona.

TEDH, Caso Buturaga vs. Rumanía, Sentencia de 11 de febrero de 2020

94. [...] En el contexto de la violencia doméstica, la cibervigilancia es a menudo llevada a cabo por la pareja íntima de la persona [...]. En consecuencia, el Tribunal acepta el argumento del demandante de que acciones como vigilar, acceder o guardar ilícitamente la correspondencia de la pareja pueden ser tenidas en cuenta por las autoridades nacionales al investigar casos de violencia doméstica.

CIBERACECHO O CIBERVIGILANCIA

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

[R]astreo constante de las actividades en línea y fuera de línea de una víctima, así como de su ubicación, desplazamientos e información a través del uso de las TIC.

Algunas de las conductas que puede incluir son:

- Utilización de software espía en dispositivos electrónicos, sin el consentimiento de la usuaria, que permiten el control remoto de cámaras o micrófonos en teléfonos móviles, o el monitoreo clandestino de llamadas y mensajes.
- Revisión constante y acceso no consentido a mensajes de texto, correos electrónicos y/o cuentas de redes sociales.
- Uso de geolocalizadores para rastrear la ubicación de una mujer sin su consentimiento, los cuales pueden estar ubicados en automóviles, bolsas de mano o juguetes de hijas/os, o rastreo de publicaciones en redes sociales para conocer la localización de la víctima.
- Uso de cámaras de vigilancia, asistentes virtuales o dispositivos inteligentes conectados en el IoT (Internet de las Cosas) para el monitoreo de las actividades de la víctima.
- Uso de servicios en la nube como iCloud o cuentas de Google para saber a qué tiene acceso la víctima y conocer sus movimientos.
- Instalación y/o uso de aplicaciones para monitorear las actividades en línea, incluyendo aplicaciones de 'control parental'.
- Obligar a una víctima a mostrar información, compartir contraseñas y claves personales de dispositivos y cuentas o al envío constante de su geolocalización.
- Control sobre amistades, comentarios, publicaciones o interacciones en redes sociales.
- Ciberespionaje de Estado en contra de mujeres con un perfil público, defensoras de derechos humanos, activistas y periodistas. (Pág. 34)

CIBERHOSTIGAMIENTO

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[C]omisión reiterada por parte de una misma persona, de actos abusivos y perturbadores a través del uso de las TIC, con el objetivo de hostigar, intimidar, acechar, molestar, controlar, atacar, humillar, amenazar, asustar, ofender o abusar verbalmente a una víctima. Estos actos pueden o no considerarse inocuos u ofensivos individualmente, sin embargo, en conjunto conforman un patrón digital de abuso que merma la sensación de seguridad de la víctima y le provoca miedo, angustia o alarma. (Pág. 29)

El ciberhostigamiento puede abarcar las siguientes conductas:

Actos reiterados de hostigamiento, asedio, persecución digital, ataques, humillación, amenazas, ofensas u abusos a través de correos electrónicos, llamadas, mensajes de texto, chats en línea o plataformas de redes sociales.

Comentarios repetitivos en línea de naturaleza obscena, vulgar, difamatoria o amenazante.

Espiar y compilar obsesivamente información en línea de una víctima y/o establecer o intentar constantemente entablar comunicación con ella en contra de su consentimiento.

Contacto y hostigamiento a través de las TIC, de la familia, amistades o colegas de una víctima de violencia de género con el objeto de acceder a ella.

Envío constante de solicitudes de amistad en redes sociales, o unirse a todos los grupos online de los que la víctima forma parte.

Seguimiento obsesivo de publicaciones en redes sociales de la víctima a través de amistades o familiares.

Mensajes amenazantes o que busquen mantener el control de las interacciones digitales de la víctima.

Formulación de proposiciones sexuales indeseadas, reiteradas, o envío de fotos con contenido sexual sin autorización.

Monitoreo, persecución, búsqueda de cercanía física o vigilancia constante de la ubicación, actividades o comunicaciones de la víctima para que ésta lo note.

Publicación constante de información falsa u ofensiva de una persona en sus redes sociales, blogs o sitios web, o distribución de fotos íntimas o videos en plataformas de internet o a través del teléfono móvil. (Pág. 29)

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, Informe de 18 de junio de 2018

38. El acoso moral y el hostigamiento en línea son los equivalentes en Internet del acoso moral en el trabajo o el hostigamiento en plataformas sociales, Internet, salas de chat, mensajería instantánea y comunicaciones móviles.

39. El hostigamiento criminal en línea es el acoso reiterado de personas, perpetrado por medio de teléfonos móviles o aplicaciones de mensajería, en forma de llamadas de broma o conversaciones privadas mediante aplicaciones en línea (como WhatsApp) o grupos de chat en línea.

(En el mismo sentido: Oficina de Naciones Unidas para la Droga y el Delito (UNODC), Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, de 2015, pág. 12).

CIBERACOSO

Ley 14811, de 12 de enero de 2024 (Brasil)

Artículo 6:

Intimidación sistemática (***bullying***)

Artículo 146-A. Intimidar sistemáticamente, individualmente o en grupo, mediante violencia física o psicológica, a una o más personas, de forma intencionada y repetitiva, sin motivación evidente, mediante actos de intimidación, humillación o discriminación o acciones verbales, morales, sexuales, sociales, psicológicas, físicas, materiales. o virtuales:

Pena - multa, si la conducta no constituye un delito más grave.

Intimidación virtual sistemática (***cyberbullying***)

Párrafo único. Si la conducta se realiza a través de una red informática, red social, aplicaciones, juegos en línea o cualquier otro medio o entorno digital, o se transmite en tiempo real:

Pena - prisión de 2 (dos) años a 4 (cuatro) años, y multa, si la conducta no constituye delito más grave.

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[...] En términos generales implica el uso de las TIC para abusar, humillar, molestar, atacar, amenazar, degradar, intimidar ofender y/o insultar a una persona por razones de género, creando un ambiente ofensivo y hostil en los espacios digitales. A diferencia del ciberhostigamiento en el que hay un patrón de comportamientos abusivos realizados por un agresor, en el caso del ciberacoso basta la existencia de un solo incidente para que éste se verifique (si bien puede estar conformado por diversos incidentes), y puede realizarse por múltiples agresores de forma coordinada o esporádica. (Pág. 30)

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, Informe de 18 de junio de 2018

40. El acoso sexual en línea se refiere a toda forma de conducta verbal o no verbal indeseada de naturaleza sexual que tiene por objetivo o consecuencia atentar contra la dignidad de la persona y en particular crear un entorno intimidatorio, hostil, degradante, humillante u ofensivo.

(En el mismo sentido: Consejo de Europa, Comité de la Convención sobre Delitos Cibernéticos, Grupo de Trabajo sobre ciberacoso y otras formas de violencia en línea, especialmente contra mujeres y niños, "Estudio de mapeo sobre ciberviolencia", de 9 de julio de 2018, págs. 7-11)

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

Artículo 7. Ciberacoso.

Los Estados miembros garantizarán que las siguientes conductas intencionadas sean punibles como delito:

CIBERACOSO

g) la participación reiterada o continua en conductas amenazantes dirigidas contra otra persona, al menos cuando esa conducta implique amenazas de cometer delitos, mediante TIC, y cuando sea probable que cause en la persona un profundo temor por su propia seguridad o por la seguridad de las personas a cargo;

h) la participación, junto con otras personas, mediante TIC, en conductas amenazantes o insultantes accesibles públicamente dirigidas contra una persona, cuando sea probable que tal conducta cause graves daños psicológicos a esa persona;

i) el envío no solicitado a una persona, mediante TIC, de una imagen, vídeo u otro material similar que represente los genitales, cuando sea probable que tal conducta cause daños psicológicos a esa persona;

j) hacer accesible al público, mediante TIC, material que contenga los datos personales de una persona, sin su consentimiento, con el fin de incitar a terceros a causar lesiones físicas o psicológicas graves a dicha persona.

(En el mismo sentido: Comité CEDAW, Recomendación general nº 36 sobre el derecho de las niñas y las mujeres a la educación, de 27 de noviembre de 2017, párrs. 70 y ss).

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

37. Según el artículo 40 del Convenio de Estambul, el acoso sexual constituye "cualquier forma de conducta verbal, no verbal o física no deseada de naturaleza sexual que tenga por objeto o efecto violar la dignidad de una persona, en particular cuando cree un ambiente intimidante, hostil, degradante, humillante u ofensivo".

38. Esta Recomendación General considera bajo esta definición los siguientes comportamientos en línea o a través de medios digitales:

[...]

(b) la toma, producción o obtención de imágenes o vídeos íntimos sin consentimiento incluye actos de «upskirting» y toma de «creepshots», así como la producción de imágenes alteradas digitalmente en las que el rostro o el cuerpo de una persona se superpone o «cose» en una imagen pornográfica. fotografía o vídeo, conocida como "pornografía falsa" (como los "deepfakes", cuando se crean imágenes sintéticas mediante inteligencia artificial);

(c) la explotación, la coerción y las amenazas comprendidas en el ámbito del artículo 40 del Convenio incluyen formas de violencia como el *sexting* forzado, la extorsión sexual, las amenazas de violación, el *doxing* sexualizado/de género, la suplantación de identidad y el *outing*;

(d) el acoso sexualizado constituye comportamientos tales como hacer circular chismes o rumores sobre el presunto comportamiento sexual de una víctima, publicar comentarios sexualizados debajo de las publicaciones o fotografías de la víctima, hacerse pasar por una víctima y compartir contenido sexual o acosar sexualmente a otros, afectando así a su reputación y/o sus medios de vida. , o "sacar a la luz" a alguien sin su consentimiento con el propósito de asustarlo, amenazarlo y avergonzarlo; y

(e) el *cyberflashing* consiste en el envío de imágenes sexuales no solicitadas a través de aplicaciones de citas o mensajería, mensajes de texto o mediante el uso de tecnologías Airdrop o Bluetooth.

GROOMING

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[A]cción deliberada de un adulto de contactar a una persona menor de edad, a través de medios electrónicos o cualquier otra tecnología de transmisión de datos, con el objeto de ganar su confianza, atacar su integridad sexual o con fines de explotación sexual (incluyendo la obtención, almacenamiento o difusión de pornografía infantil). El ***grooming*** puede hacerse a través de redes sociales, chats de mensajería instantánea o juegos en línea. (Pág. 36)

Código Penal de la Nación Argentina

Artículo 131.

Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma.

Código Penal de Uruguay

Artículo 321.bis

El que, mediante la utilización de tecnologías, de internet, de cualquier sistema informático o cualquier medio de comunicación o tecnología de transmisión de datos, contactare a una persona menor de edad o ejerza influencia sobre el mismo, con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener material pornográfico u obligarlo a hacer o no hacer algo en contra de su voluntad será castigado con de seis meses de prisión a cuatro años de penitenciaría.

Código Penal de España

Artículo 183

1. El que a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo a fin de cometer cualquiera de los delitos descritos en los artículos 181 y 189, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será castigado con la pena de uno a tres años de prisión o multa de doce a veinticuatro meses, sin perjuicio de las penas correspondientes a los delitos en su caso cometidos. Las penas se impondrán en su mitad superior cuando el acercamiento se obtenga mediante coacción, intimidación o engaño.

2. El que, a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor, será castigado con una pena de prisión de seis meses a dos años.

CREACIÓN, DIFUSIÓN, PUBLICACIÓN, DISTRIBUCIÓN, INTERCAMBIO, MANIPULACIÓN O ALMACENAMIENTO DE FOTOGRAFÍAS, VIDEOS O AUDIOS DE NATURALEZA SEXUAL O ÍNTIMA SIN CONSENTIMIENTO

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[E]lementos:

- Existencia de material audiovisual (real o editado) de carácter íntimo y/o sexual;
- Creación, almacenamiento, manipulación o producción, difusión, publicación, distribución, facilitación, cesión o entrega a terceros de este material;
- Intermediación de las TIC (uso de cualquier tipo de comunicación electrónica, de transmisión de datos, plataforma de internet y/o de cualquier otro medio de comunicación); y
- Falta de consentimiento de la persona que aparece en ese material. Sobre este punto, es importante destacar la existencia de dos posibles escenarios: que no haya consentimiento para la obtención y publicación del material audiovisual íntimo; o que la obtención del material audiovisual haya sido acordada, pero que no haya consentimiento para su publicación o difusión.

El MESECVI llama la atención sobre el hecho de que a la distribución no consensuada de material íntimo se le ha denominado comúnmente "pornovenganza", si bien este es un término reductivo y problemático al no reflejar la diversidad de motivaciones de los perpetradores, las cuales se extienden más allá de la venganza y pueden incluir desde una reafirmación de su masculinidad hasta la extorsión económica o su gratificación sexual. Además, el uso de este término minimiza el daño que estos actos causan a las víctimas al ocultar el componente no consensual de la conducta y colocar énfasis en el material íntimo en lugar del comportamiento abusivo de los perpetradores. (Págs. 31-32).

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

23. [L]a "pornografía vengativa" consiste en la difusión en línea no consensuada de imágenes íntimas, obtenidas con o sin consentimiento, con el fin de avergonzar, estigmatizar o dañar a la víctima [...].

(En el mismo sentido: Consejo de Europa, Comité de la Convención sobre Delitos Cibernéticos, Grupo de Trabajo sobre ciberacoso y otras formas de violencia en línea, especialmente contra mujeres y niños, "Estudio de mapeo sobre ciberviolencia", de 9 de julio de 2018, págs. 9-10; 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, Informe de 18 de junio de 2018, párr. 41).

Código Penal Federal (México)

Artículo 199 octies.

Comete el delito de violación a la intimidad sexual, aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización.

Así como quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización.

Estas conductas se sancionarán con una pena de tres a seis años de prisión y una multa de quinientas a mil Unidades de Medida y Actualización.

Artículo 199 nonies.

CREACIÓN, DIFUSIÓN, PUBLICACIÓN, DISTRIBUCIÓN, INTERCAMBIO, MANIPULACIÓN O ALMACENAMIENTO DE FOTOGRAFÍAS, VIDEOS O AUDIOS DE NATURALEZA SEXUAL O ÍNTIMA SIN CONSENTIMIENTO

Se impondrán las mismas sanciones previstas en el artículo anterior cuando las imágenes, videos o audios de contenido íntimo sexual que se divulguen, compartan, distribuyan o publiquen no correspondan con la persona que es señalada o identificada en los mismos.

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 8 de marzo de 2024

Artículo 5. Difusión no consentida de material íntimo o manipulado.

1. Los Estados miembros garantizarán que sean punibles como delito las siguientes conductas intencionadas:

a) hacer accesible al público, mediante tecnologías de la información y de las comunicaciones (TIC), imágenes, vídeos o materiales similares que representen actividades sexualmente explícitas o las partes íntimas de una persona sin su consentimiento, cuando sea probable que tal conducta cause graves daños a esa persona;

b) producir, manipular o alterar y, posteriormente, hacer accesible al público, mediante TIC, imágenes, vídeos o materiales similares, haciendo que parezca que una persona está practicando actividades sexualmente explícitas, sin el consentimiento de dicha persona, cuando sea probable que tal conducta cause graves daños a esa persona; [...]

(En el mismo sentido: GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, párr. 38.a).

Código Penal de Perú

Artículo 154.

El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de libertad no mayor de dos años.

La pena será no menor de uno ni mayor de tres años y de treinta a ciento veinte días-multa, cuando el agente revela la intimidad conocida de la manera antes prevista

Si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de sesenta a ciento ochenta días-multa.

[...]

Artículo 154-B. Difusión de imágenes, materiales audiovisuales o audios con contenido sexual.

El que, sin autorización, difunde, revela, publica, cede o comercializa imágenes, materiales audiovisuales o audios con contenido sexual de cualquier persona, que obtuvo con su anuencia, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años y con treinta a ciento veinte días-multa.

La pena privativa de libertad será no menor de tres ni mayor de seis años y de ciento ochenta a trescientos sesenta y cinco días-multa, cuando concurra cualquiera de las siguientes circunstancias:

1) Cuando la víctima mantenga o haya mantenido una relación de pareja con el agente, son o han sido convivientes o cónyuges.

2) Cuando para materializar el hecho utilice redes sociales o cualquier otro medio que genere una difusión masiva.

AMENAZAS DIRECTAS DE DAÑO O DE VIOLENCIA

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

[E]nvío o publicación de comunicaciones o contenidos digitales que le anticipan a una persona la intención de cometer en su contra un daño físico o violencia sexual, o en contra de sus familiares, amistades o bienes.

Esta forma de ciberviolencia incluye actos como:

Envío o publicación de mensajes de correo electrónico o redes sociales, imágenes o videos anunciando un peligro inminente o violencia sexual.

Extorsión digital, que involucra el uso de las TIC para ejercer presión sobre una persona a fin de forzarla a actuar de cierto modo u obtener dinero.

Amenazas de difundir o enviar a familiares de la víctima información privada para su explotación o chantaje sexual.

Sextorsión, que conlleva la utilización de material íntimo como un elemento de control sobre la víctima. Implica la realización de amenazas, chantaje o extorsión sexual que se le hace a una persona, previamente filmada o fotografiada desnuda o realizando actos sexuales, de difundir ese material a cambio de dinero, para exigirle que entregue más material audiovisual íntimo o para obligarla a mantener relaciones sexuales. (Pág. 35)

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 8 de marzo de 2024

Artículo 5. Difusión no consentida de material íntimo o manipulado.

1. Los Estados miembros garantizarán que sean punibles como delito las siguientes conductas intencionadas:

[...]

c) amenazar con cometer las conductas mencionadas en las letras a) o b) con el fin de coaccionar a una persona para que realice o acceda a que se realice determinado acto o se abstenga de realizarlo.

Código Penal de la Ciudad de México

Artículo 209.

Al que amenace a otro con causarle un mal en su persona, bienes, honor o derechos, o en la persona, honor, bienes o derechos de alguien con quien esté ligado por algún vínculo, se le impondrá de tres meses a un año de prisión o de noventa a trescientos sesenta días multa.

La pena se agravará al triple cuando la amenaza consista en difundir, exponer, distribuir, publicar, compartir, exhibir, reproducir, intercambiar, ofertar, comerciar o transmitir, mediante materiales impresos, correo electrónico, mensaje telefónico, redes sociales o cualquier medio tecnológico; imágenes, audios o videos de contenido sexual íntimo de una persona sin su consentimiento u obtenido mediante engaño.

EXTORSIÓN

Se entenderá como personas ligadas por algún vínculo con la víctima:

a) A las personas ascendientes y descendientes consanguíneas o afines;

b) La persona cónyuge, la concubina, el concubinario, pareja permanente y parientes colaterales por consanguinidad hasta el cuarto grado y por afinidad hasta el segundo; y

c) Las personas que estén ligadas con las víctimas por amor, respeto, gratitud o estrecha amistad. Este delito se perseguirá por querella.

Artículo 236.

Al que obligue a otro a dar, hacer, dejar de hacer o tolerar algo, obteniendo un lucro para sí o para otro causando a alguien un perjuicio patrimonial, se le impondrán de cinco a diez años de prisión y de mil a dos mil unidades de medida y actualización. [...]

Asimismo, las penas se incrementarán en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica y cuando el delito emplee imágenes, audios o videos de contenido sexual íntimo.

(En el mismo sentido: GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, párr. 38.a).

SUPLANTACIÓN Y ROBO DE IDENTIDAD EN LÍNEA

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

Consiste en la utilización de la imagen, información o datos de una persona, o la creación de una identidad falsa con la imagen o datos de una persona, sin mediar su consentimiento y a través del uso de las TIC, con el fin de amenazarla, intimidarla o dañar su reputación.

Esta forma de violencia puede involucrar lo siguiente:

- Creación de perfiles o cuentas falsas en redes sociales o de cuentas de correo electrónico que utilizan la información o imagen de una persona u organización.
- Usurpación de cuentas de correo electrónico o números de teléfono para contactar, en nombre de la víctima, a sus amistades, familiares, centros laborales, o compañeras/os de trabajo.
- Eliminar, enviar o manipular mensajes de correo electrónico o contenido en línea sin el consentimiento de la víctima.
- Robo de dinero o realizar compras en línea a partir del robo de datos bancarios. (Pág. 34)

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

41. [...] Los perpetradores también pueden asumir la identidad de la otra persona o monitorear a la víctima a través de dispositivos tecnológicos conectados a través del Internet de las Cosas (IoT), como electrodomésticos inteligentes.

Código Penal de España

Artículo 172 ter.5

El que, sin consentimiento de su titular, utilice la imagen de una persona para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contacto o cualquier medio de difusión pública, ocasionándole a la misma situación de acoso, hostigamiento o humillación, será castigado con pena de prisión de tres meses a un año o multa de seis a doce meses. Si la víctima del delito es un menor o una persona con discapacidad, se aplicará la mitad superior de la condena.

TRÁFICO ILEGAL DE DATOS PERSONALES

Código Penal de Perú

Artículo 154-A. Tráfico ilegal de datos personales.

El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior.

HACKEO DE DISPOSITIVOS INFORMÁTICOS

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

Esta forma de violencia digital puede incluir, entre otras, las siguientes conductas:

- Ataques a cuentas en línea o dispositivos para acceder sin autorización a fin de obtener información mediante robo de contraseñas, hackeo, instalación de software espía, *keyloggers* o control remoto de webcams o micrófonos.
- Manipulación y control de dispositivos, incluyendo la obstrucción de acceso y el *bluejacking*.
- Uso, manipulación y modificación no consentida de información (eliminar, modificar o falsificar datos personales, incluyendo fotos y videos).
- Obtención de datos personales mediante *phishing* o *pharming*.
- Revelación de la identidad o preferencia sexual de una persona (*outing*), incluyendo exposición de mujeres o integrantes de la comunidad LGTBIQ+ mediante la publicación de sus certificados de nacimiento.
- Bloqueo de acceso a cuentas en línea o cuentas de correo electrónico y control de las mismas así como de la información personal de una víctima.
- En cuanto al *doxing*, este puede consistir en la publicación sin consentimiento de la ubicación de la víctima o de la geologalización automática por plataformas de redes sociales o aplicaciones. (Pág. 34)

Código Penal Federal de la Ciudad de México

Artículo 334.

A quien intervenga comunicaciones privadas sin mandato de autoridad judicial competente, se le impondrán de dos a ocho años de prisión y de cien a mil días multa. A quien revele, divulgue, utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le impondrán de tres a doce años de prisión y de doscientos a mil días multa.

Asimismo, las penas se incrementarán en una mitad cuando se utilice como medio comisivo la vía telefónica, el correo electrónico o cualquier otro medio de comunicación electrónica y cuando el delito emplee imágenes, audios o videos de contenido sexual íntimo.

Ley nº 12.737 (Ley Carolina Dickerman - Brasil), de 30 de noviembre de 2012

Artículo 2.

Artículo 154-A. Irrumpir en el dispositivo informático de otra persona, esté o no conectado a la red informática, mediante violación indebida de un mecanismo de seguridad y con el objetivo de obtener, alterar o destruir datos o información sin la autorización expresa o tácita del titular del dispositivo o instalar vulnerabilidades. para obtener una ventaja ilícita:

Pena - detención, de 3 (tres) meses a 1 (un) año, y multa.

§ 1 Incurre en la misma pena quien produzca, ofrezca, distribuya, venda o difunda un dispositivo o programa de ordenador con la intención de permitir la práctica de la conducta definida en el caput.

HACKEO DE DISPOSITIVOS INFORMÁTICOS

§ 2 La pena se aumentará de un sexto a un tercio si la invasión produce pérdidas económicas.

§ 3º Si la invasión tiene como resultado la obtención de contenidos de comunicaciones electrónicas privadas, secretos comerciales o industriales, información confidencial, tal como la define la ley, o el control remoto no autorizado del dispositivo invadido:

Pena - prisión, de 6 (seis) meses a 2 (dos) años, y multa, si la conducta no constituye delito más grave.

§ 4 En el caso del § 3, la pena aumenta de uno a dos tercios si hay divulgación, comercialización o transmisión a un tercero, a cualquier título, de los datos o de la información obtenidos. [...]

EXPLOTACIÓN SEXUAL Y/O TRATA DE MUJERES Y NIÑAS FACILITADA POR LAS TECNOLOGÍAS

Consejo de Europa, Comité de la Convención sobre Delitos Cibernéticos, Grupo de Trabajo sobre ciberacoso y otras formas de violencia en línea, especialmente contra mujeres y niños, "Estudio de mapeo sobre ciberviolencia", de 9 de julio de 2018

Los niños y niñas parecen representar un grupo primario de víctimas de la ciberviolencia, en particular con respecto a la violencia sexual en línea. Si bien la "explotación sexual y el abuso sexual de niños en línea" no son necesariamente formas nuevas y distintas de explotación y abuso sexual de niños y niñas, las TIC han aumentado el acceso a los niños y a las niñas por parte de personas que buscan abusar y explotar sexualmente de ellos. Las TIC facilitan el intercambio de información Las imágenes y vídeos del abuso sexual y, por lo tanto, refuerzan el impacto dañino y duradero del abuso de niños y niñas. Las TIC también contribuyen a facilitar las ganancias comerciales de la explotación sexual de niños y niñas. tipos de delitos sexuales contra niños. [...]

(En el mismo sentido: OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022, pág. 36).

Convenio sobre ciberdelincuencia de Budapest, de 23 de noviembre de 2001

Artículo 9. Delitos relacionados con la pornografía infantil.

1. 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 de pornografía infantil con la intención de difundirla a través de un sistema informático;

b) La oferta o puesta a disposición de pornografía infantil a través de un sistema informático;

c) La difusión o la transmisión de pornografía infantil a través de un sistema informático;

d) La adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático.

e) La posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por "pornografía infantil" todo material pornográfico que contenga la representación visual de:

a) Un menor adoptando un comportamiento sexualmente explícito.

b) Una persona que parezca menor adoptando un comportamiento sexualmente explícito.

c) Imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del párrafo 2 anterior, se entenderá por "menor" toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años. [...]

EXPLOTACIÓN SEXUAL Y/O TRATA DE MUJERES Y NIÑAS FACILITADA POR LAS TECNOLOGÍAS

Código Penal de la Ciudad de México (modificado por la Ley Olimpia-México)

Artículo 183. Corrupción de menores.

Al que comercie, distribuya, exponga, haga circular u oferte, a menores de dieciocho años de edad o personas que no tengan la capacidad de comprender el significado del hecho o de personas que no tienen capacidad de resistir la conducta, libros, escritos, grabaciones, filmes, fotografías, anuncios impresos, imágenes u objetos, de carácter lascivo o sexual, reales o simulados, sea de manera física, o a través de cualquier medio, se le impondrá de uno a cinco años de prisión y de quinientos a mil días multa.

Artículo 187. Pornografía infantil.

[...]

Al que fije, imprima, video grabe, audio grabe, fotografíe, filme o describa actos de exhibicionismo corporal o lascivos o sexuales, reales o simulados, en que participe una persona menor de dieciocho años de edad o persona que no tenga la capacidad de comprender el significado del hecho o de persona que no tiene capacidad de resistir la conducta, se le impondrá la pena de siete a doce años de prisión y de mil a dos mil días multa, así como el decomiso y destrucción de los objetos, instrumentos y productos del delito.

Se impondrán las mismas sanciones a quien financie, elabore, reproduzca, almacene, distribuya, comercialice, arriende, exponga, publicite, difunda, adquiera, intercambie o comparta por cualquier medio el material a que se refieren las conductas anteriores. Al que permita directa o indirectamente el acceso de un menor a espectáculos, obras gráficas o audiovisuales de carácter lascivo o sexual, se le impondrá prisión de uno a tres años y de cincuenta a doscientos días multa.

Código Penal de la Nación Argentina

Artículo 128.

Será reprimido con prisión de tres (3) a seis (6) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.
Será reprimido con prisión de cuatro (4) meses a un (1) año el que a sabiendas tuviere en su poder representaciones de las descriptas en el párrafo anterior.

Será reprimido con prisión de seis (6) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el primer párrafo con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.
Todas las escalas penales previstas en este artículo se elevarán en un tercio en su mínimo y en su máximo cuando la víctima fuere menor de trece (13) años.

INCITACIÓN A LA VIOLENCIA O AL ODIO POR MEDIOS CIBERNÉTICOS

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

(Considerando 26) El delito de incitación a la violencia o al odio por medios cibernéticos presupone que la incitación no se expresa en un contexto puramente privado, sino públicamente mediante TIC. Por lo tanto, un requisito para que exista debe ser la difusión al público, que debe entenderse como hacer accesible, mediante TIC, un determinado elemento del material que incite a la violencia o al odio a un número potencialmente ilimitado de personas, es decir, hacer que el material sea fácilmente accesible para los usuarios en general, sin que sea necesario que la persona que lo haya facilitado haga nada más, y con independencia de que esas personas accedan de hecho a la información en cuestión. En consecuencia, cuando el acceso al material exija el registro o la admisión en un grupo de usuarios, debe considerarse que existe difusión al público únicamente cuando los usuarios que intenten acceder al material sean automáticamente registrados o admitidos sin que un ser humano decida o seleccione a quién se otorga el acceso. Al evaluar si un material puede ser considerado constitutivo de incitación al odio o a la violencia, las autoridades competentes deben tener en cuenta el derecho fundamental a la libertad de expresión consagrado en el artículo 11 de la Carta.

Artículo 8. Incitación a la violencia o al odio por medios cibernéticos.

1. Los Estados miembros garantizarán que sea punible como delito incitar intencionadamente a la violencia o al odio contra un grupo de personas o un miembro de dicho grupo, definido por referencia al género, publicando, mediante TIC, material que contenga esa incitación.

2. A los efectos de lo dispuesto en el apartado 1, los Estados miembros podrán optar por castigar únicamente las conductas que o bien se lleven a cabo de forma que sea probable que perturben el orden público, o bien sean amenazantes, abusivas o insultantes.

ACNUDH, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", de 24 de junio de 2020

15. A pesar de su positivo y transformador potencial, el uso de las TIC también ha permitido un discurso de odio y un discurso peligroso en contra de ciertos grupos raciales y religiosos, así como la discriminación, las agresiones y la violencia por motivos de género, en particular la violencia contra las mujeres y las niñas. Esta situación suele reflejar y puede exacerbar una serie de estereotipos raciales y de género nocivos, la discriminación y la violencia fuera de la Red. La violencia en la Red contra ciertas minorías raciales y religiosas y contra las mujeres y las niñas ha experimentado un brusco aumento en los últimos años y puede conllevar una limitación de la participación de las mujeres en las plataformas digitales. Esta conclusión es especialmente manifiesta cuando son activistas de derechos civiles e igualdad racial y grupos de mujeres y niñas los que organizan las reuniones. Los actos de violencia y maltrato en la Red contra minorías raciales y religiosas y contra las mujeres y las niñas provoca que muchos se practiquen la autocensura o limiten sus interacciones en línea, lo que supone una restricción del ejercicio de sus derechos, en particular el derecho a la libertad de reunión pacífica. Las singularidades raciales y de género y las posibilidades que brindan las TIC para intimidar, amenazar y lesionar a las mujeres y las niñas, incluso fuera de la Red, exigen una reflexión cuidadosa y profunda, así como medidas específicas de reacción.

(En el mismo sentido: Consejo de Europa, Comité de la Convención sobre Delitos Cibernéticos, Grupo de Trabajo sobre ciberacoso y otras formas de violencia en línea, especialmente contra mujeres y niños, "Estudio de mapeo sobre ciberviolencia", de 9 de julio de 2018, pág. 13; OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022, pág. 36).

INCITACIÓN A LA VIOLENCIA O AL ODIO POR MEDIOS CIBERNÉTICOS

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

32. [R]ecuerda que la práctica de etiquetar a las personas LGBTIQ como una «ideología» se está extendiendo en la comunicación en línea y fuera de línea y en campañas contra la denominada «ideología de género»; destaca que feministas y activistas LGBTIQ son a menudo objeto de campañas de difamación, incitación al odio en línea y ciberacoso;

2.4 El papel y responsabilidad de los intermediarios

EL PAPEL Y RESPONSABILIDAD DE LOS INTERMEDIARIOS

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

[A]lgunos intermediarios han desarrollado diversas políticas para atender los incidentes de violencia de género contra las mujeres y las niñas, como, por ejemplo, mediante el bloqueo de agresores o la eliminación de contenidos. Sin embargo, en general, las respuestas de los intermediarios de internet frente a la violencia de género son aún insuficientes en la región.(Pág. 96)

A partir de un análisis de reportes de organizaciones de la sociedad civil, se han observado las siguientes problemáticas en el actuar de los intermediarios de internet frente a la violencia de género contra las mujeres: una falta de reconocimiento de las experiencias de violencia que viven las mujeres en América Latina y el Caribe, concentrando usualmente sus políticas en la situación de las mujeres que habitan en Norteamérica o Europa; un control inadecuado de los contenidos violentos contra las mujeres; una ausencia de canales adecuados para que éstas puedan reportar contenidos abusivos y solicitar su remoción (con formularios de reporte confusos, poco visibles y que no se adaptan a las necesidades regionales o a los idiomas locales); una falta de respuesta oportuna de las denuncias presentadas, las cuales no se atienden de forma oportuna o son desestimadas argumentando que no violan las normas comunitarias; una falta de transparencia respecto del sistema de moderación de contenidos; y estándares débiles de protección de la privacidad y seguridad digitales de las usuarias. (Pág. 97)

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, Informe, de 18 de junio de 2018

71. El papel de los intermediarios privados en la regulación y gobernanza de Internet ha sido objeto de escrutinio progresivo, habida cuenta de que la violencia en línea por razón de género suele perpetrarse en plataformas de propiedad privada, que con frecuencia se utilizan en distintas jurisdicciones. Los intermediarios de Internet desempeñan un papel fundamental en el suministro de espacios digitales para la interacción y, como tales, tienen responsabilidades específicas en materia de derechos humanos. Sin embargo, estas responsabilidades, aún no se han examinado plenamente en el marco internacional de derechos humanos; por ejemplo, si bien en los Principios Rectores sobre las Empresas y los Derechos Humanos se afirma la responsabilidad de las empresas de respetar los derechos humanos en general, no se hace ninguna referencia directa a la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer u otros instrumentos relativos a los derechos de la mujer.

72. Los intermediarios de Internet, todas las empresas de almacenamiento de datos de clientes y las que proporcionan almacenamiento en la nube también tienen el deber de cumplir con las normas de derechos humanos manteniendo los datos seguros, y deben rendir cuentas de la piratería de los datos si no cuentan con las salvaguardias suficientes.

EL PAPEL Y RESPONSABILIDAD DE LOS INTERMEDIARIOS

73. [L]as respuestas inadecuadas y deficientes de los intermediarios sobre violencia en línea por razón de género pueden tener un efecto negativo en la libertad de expresión, lo que da lugar a la censura por las plataformas, la autocensura o la censura por otros usuarios, y no proporciona a las víctimas de acoso ninguna forma de reparación.

Ley Nº 12.965, que establece principios, garantías, derechos y deberes para el uso de internet (Brasil), de 23 de abril de 2014

Artículo 21.

El proveedor de aplicaciones de Internet que ponga a disposición contenidos generados por terceros será responsable subsidiario de la violación de la privacidad resultante de la difusión, sin la autorización de sus participantes, de imágenes, videos u otros materiales que contengan escenas de desnudez o desnudez. actos sexuales de carácter privado cuando, previa notificación por parte del participante o de su representante legal, no promueva diligentemente, dentro del alcance y límites técnicos de su servicio, la indisponibilidad de dichos contenidos.

2.5 La inteligencia artificial

LOS USOS DE LA INTELIGENCIA ARTIFICIAL

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

16. Las herramientas de IA se utilizan profusamente para comprender los patrones de comportamiento humano. Con el acceso a los conjuntos de datos adecuados, es posible sacar conclusiones sobre el número de personas de un barrio concreto que suelen frecuentar un determinado lugar de culto, qué programas de televisión prefieren e incluso a qué hora suelen levantarse y acostarse. Estas herramientas permiten hacer deducciones de gran alcance sobre las personas, incluso sobre su estado mental y físico, y permitir la identificación de grupos de personas, por ejemplo en función de sus inclinaciones políticas o personales particulares. La IA también se utiliza para evaluar la probabilidad de comportamientos o acontecimientos futuros. Las deducciones y predicciones realizadas mediante IA, a pesar de su carácter probabilístico, pueden servir de base para la adopción de decisiones que afectan a los derechos de las personas, a veces de forma totalmente automatizada.

LA COMISIÓN DE ERRORES POR PARTE DE LOS SISTEMAS BASADOS EN LA INTELIGENCIA ARTIFICIAL

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

18. Las decisiones basadas en la IA no están exentas de errores. De hecho, la escalabilidad de las soluciones en esta esfera puede aumentar drásticamente los efectos negativos de tasas de error aparentemente bajas. Los resultados erróneos de los sistemas de IA proceden de diversas fuentes. Para empezar, los resultados de los algoritmos de IA tienen elementos probabilísticos, lo que significa que sus resultados albergan un margen de incertidumbre. Además, a menudo la pertinencia y la exactitud de los datos resultan cuestionables. Por otra parte, las expectativas poco realistas pueden llevar a que se implanten herramientas de IA que no están preparadas para producir los objetivos deseados. Por ejemplo, en la esfera médica, un análisis de cientos de herramientas para el diagnóstico y la prevención de la COVID-19, cuyo desarrollo había suscitado grandes expectativas, reveló que ninguna de ellas resultaba apta para el uso clínico.

19. Los resultados de los sistemas de IA que se basan en datos erróneos pueden contribuir de muchas formas a la vulneración de derechos humanos por ejemplo, señalando erróneamente a una persona como posible terrorista o indicando que ha cometido un fraude en el cobro de prestaciones sociales. Resultan especialmente preocupantes los conjuntos de datos sesgados que conducen a decisiones discriminatorias basadas en sistemas de IA.

LA OPACIDAD DE LOS MECANISMOS DE TOMA DE DECISIÓN EN LA INTELIGENCIA ARTIFICIAL

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

18. Las decisiones basadas en la IA no están exentas de errores. De hecho, la escalabilidad de las soluciones en esta esfera puede aumentar drásticamente los efectos negativos de tasas de error aparentemente bajas. Los resultados erróneos de los sistemas de IA proceden de diversas fuentes. Para empezar, los resultados de los algoritmos de IA tienen elementos probabilísticos, lo que significa que sus resultados albergan un margen de incertidumbre. Además, a menudo la pertinencia y la exactitud de los datos resultan cuestionables. Por otra parte, las expectativas poco realistas pueden llevar a que se implanten herramientas de IA que no están preparadas para producir los objetivos deseados. Por ejemplo, en la esfera médica, un análisis de cientos de herramientas para el diagnóstico y la prevención de la COVID-19, cuyo desarrollo había suscitado grandes expectativas, reveló que ninguna de ellas resultaba apta para el uso clínico.

19. Los resultados de los sistemas de IA que se basan en datos erróneos pueden contribuir de muchas formas a la vulneración de derechos humanos por ejemplo, señalando erróneamente a una persona como posible terrorista o indicando que ha cometido un fraude en el cobro de prestaciones sociales. Resultan especialmente preocupantes los conjuntos de datos sesgados que conducen a decisiones discriminatorias basadas en sistemas de IA.

LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL EN MATERIA DE SEGURIDAD, JUSTICIA Y GESTÓN DE FRONTERAS

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

23. Los sistemas de IA se utilizan a menudo como herramientas de predicción. Estas aplican algoritmos para analizar grandes cantidades de datos, incluidos datos históricos, a fin de evaluar los riesgos y predecir las tendencias futuras. En función de cuál sea la finalidad, los datos de formación y los datos analizados pueden incluir, por ejemplo, antecedentes penales, actas de detención, estadísticas sobre delincuencia, informes de intervenciones policiales en barrios específicos, publicaciones en medios sociales, datos de comunicaciones y registros de viajes. Las tecnologías pueden utilizarse para crear perfiles de personas, identificar lugares susceptibles de albergar una mayor actividad delictiva o terrorista, e incluso señalar a individuos como sospechosos probables y futuros reincidentes.

24. Las consecuencias de estas actividades para la privacidad y los derechos humanos en general son enormes. En primer lugar, los conjuntos de datos utilizados incluyen información sobre un gran número de personas, lo que afecta a su derecho a la privacidad. En segundo lugar, estos pueden desencadenar intervenciones del Estado, como registros, interrogatorios, detenciones y enjuiciamientos, aunque las evaluaciones de IA por sí mismas no deberían considerarse motivos razonables de sospecha dado el carácter probabilístico de las predicciones. Entre los derechos afectados se encuentran el derecho a la privacidad, el derecho a un juicio imparcial, el derecho a no ser objeto de detención y privación de libertad arbitrarias y el derecho a la vida. En tercer lugar, la opacidad inherente a las decisiones basadas en la IA plantea cuestiones especialmente apremiantes en lo que respecta la responsabilidad del Estado cuando toma como base la IA para la adopción de medidas coercitivas, más aún en las esferas en las que suele existir una falta general de transparencia, como las actividades de las fuerzas de lucha contra el terrorismo. En cuarto lugar, las herramientas de predicción conllevan un riesgo inherente de perpetuar o incluso potenciar la discriminación, al reflejar prejuicios raciales y étnicos históricos integrados en los conjuntos de datos que se utilizan, como la tendencia a la aplicación desproporcionada de medidas policiales a determinadas minorías.

EL IMPACTO PERJUDICIAL DE LA ELABORACIÓN DE PERFILES ALGORÍTMICOS EN EL RACISMO, XENOFOBIA, Y OTRAS FORMAS DE EXCLUSIÓN

Comité para la Eliminación de la Discriminación Racial (CEDR), Recomendación general nº 36, relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden, de 17 de diciembre de 2020

12. [E]l Comité observa que la utilización cada vez mayor de nuevas herramientas tecnológicas, incluida la inteligencia artificial, en ámbitos como la seguridad, el control de fronteras y el acceso a los servicios sociales, puede profundizar el racismo, la discriminación racial, la xenofobia y otras formas de exclusión. [...] Aunque es consciente de que, en algunos ámbitos, la inteligencia artificial puede contribuir a una mayor eficacia en una serie de procesos de adopción de decisiones, el Comité también comprende que existe un riesgo real de sesgo algorítmico cuando se utiliza la inteligencia artificial en la adopción de decisiones en el contexto de la aplicación de la ley. La elaboración de perfiles algorítmicos plantea serias preocupaciones y las consecuencias con respecto a los derechos de las víctimas podrían ser muy graves.

31. [...] Dada la opacidad de los análisis y la adopción de decisiones algorítmicos, en particular cuando se emplean métodos de inteligencia artificial, los resultados discriminatorios de la elaboración algorítmica de perfiles pueden ser a menudo menos obvios y más difíciles de detectar que los derivados de las decisiones humanas y, por lo tanto, más difíciles de contrarrestar. [...]

32. Hay diversos puntos de entrada a través de los cuales el sesgo se podría incorporar en los sistemas de elaboración algorítmica de perfiles, entre ellos la forma en que se diseñan los sistemas, las decisiones sobre el origen y el alcance de los conjuntos de datos con que se entrenan, los sesgos sociales y culturales que los creadores de aplicaciones pueden incorporar en esos conjuntos de datos, los modelos mismos de inteligencia artificial y la forma en que los productos del modelo de inteligencia artificial se ejecutan en la práctica. [...]

33. Surgen riesgos particulares cuando se utiliza la elaboración algorítmica de perfiles para determinar la probabilidad de que se produzcan actividades delictivas en determinadas localidades o por determinados grupos o incluso personas. La actividad policial predictiva basada en datos históricos para predecir posibles hechos futuros puede producir fácilmente resultados discriminatorios [...].

34. Se ha informado de la existencia de mecanismos similares en algunos sistemas judiciales. Al aplicar una sanción o decidir si alguien debería ir a la cárcel, quedar en libertad bajo fianza o recibir otro castigo, los Estados recurren cada vez más a la elaboración algorítmica de perfiles, con el fin de prever las posibilidades de que un individuo pueda cometer uno o varios delitos en el futuro. Las autoridades recopilan información sobre el historial delictivo del individuo, su familia y sus amigos y sus condiciones sociales, incluido su historial laboral y académico, para evaluar el grado de "peligrosidad" de la persona a partir de una puntuación proporcionada por el algoritmo, que se suele mantener confidencial. Este uso de la elaboración algorítmica de perfiles plantea problemas similares a los descritos en el párrafo.

EL IMPACTO PERJUDICIAL DE LA ELABORACIÓN DE PERFILES ALGORÍTMICOS EN EL RACIS, XENOFOBIA, Y OTRAS FORMAS DE EXCLUSIÓN

35. El uso cada vez mayor de tecnologías de reconocimiento facial y vigilancia para rastrear y controlar a determinados grupos demográficos suscita preocupación en relación con muchos derechos humanos, como el derecho a la intimidad, la libertad de reunión pacífica y de asociación, la libertad de expresión y la libertad de circulación. Están diseñadas para identificar automáticamente a las personas en función de su geometría facial, lo que permitiría elaborar perfiles de personas sobre la base de motivos de discriminación como la raza, el color, el origen nacional o étnico o el género.

ACNUDH, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", de 24 de junio de 2020

32. Además, la tecnología de reconocimiento facial puede perpetuar y amplificar la discriminación, incluso contra los afrodescendientes y otras minorías, las mujeres o las personas con discapacidad, porque puede utilizarse para el perfilado de personas sobre la base de su etnia, raza, origen nacional, género y otras características. Esta tecnología también puede dar lugar a una discriminación involuntaria, ya que su precisión depende de factores como el color de la piel o el género; de hecho, la experiencia ha demostrado que las tasas de precisión en el caso del reconocimiento de personas de piel oscura y mujeres son menores.

2.6 Los derechos humanos afectados por la violencia en línea contra las mujeres

EL DERECHO A UNA VIDA LIBRE DE VIOLENCIA EN LÍNEA

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

Una interpretación evolutiva de los artículos 3 y 6 de la Convención de Belém do Pará permite afirmar que toda mujer tiene derecho a vivir libre de violencia en sus interacciones online en los ámbitos público y privado, el cual abarca su derecho a ser libre de toda forma de discriminación en internet, a ser valorada en línea libre de estereotipos de género, y a que los Estados no sólo se abstengan de realizar conductas que violen este derecho, sino también a llevar adelante las acciones positivas necesarias para que las mujeres y niñas puedan ejercer y gozar de modo efectivo este derecho en sus interacciones digitales. (Págs. 93-94)

EL PRINCIPIO DE QUE LOS DERECHOS DE LAS PERSONAS TAMBIÉN DEBEN ESTAR PROTEGIDOS EN INTERNET

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, Informe de 18 de junio de 2018

13. Aunque los instrumentos internacionales fundamentales de derechos humanos, incluidos los relativos a los derechos de la mujer, son anteriores a las TIC, aportan un conjunto global y dinámico de derechos y obligaciones con potencial de transformación, y desempeñan un papel fundamental en la promoción y protección de los derechos humanos fundamentales, incluidos los derechos de la mujer a llevar una vida libre de violencia, a la libertad de expresión, a la privacidad, a tener acceso a la información compartida a través de las TIC, y otros derechos.

17. Habida cuenta de que los derechos de la mujer son derechos humanos y la prohibición de la violencia de género se ha reconocido como un principio del derecho internacional de los derechos humanos, los derechos humanos de la mujer amparados mediante convenciones, jurisprudencia y normas amplias regionales e internacionales deben estar protegidos en Internet, en particular mediante la prohibición de la violencia por razón de género en formas facilitadas por las TIC y en línea. [...]

(En el mismo sentido: Recomendación CM/Rec(2014)6, del Consejo de Ministros del Consejo de Europa sobre una Guía de los derechos humanos para los usuarios de Internet, de 16 de abril de 2014, párr. 1)

Declaración del Comité de Ministros del Consejo de Europa sobre los derechos humanos y el estado de derecho en la sociedad de la información, de 13 de mayo de 2005

Preámbulo: [E]l acceso limitado o la ausencia de acceso a las [tecnologías de la información y de la comunicación (TIC) puede privar a los individuos de la capacidad de ejercer plenamente sus derechos fundamentales.

EL ENFOQUE DE DERECHOS HUMANOS EN LA INTELIGENCIA ARTIFICIAL

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

38. Un enfoque de la IA basado en los derechos humanos exige la aplicación de varios principios básicos, como la igualdad y la no discriminación, la participación y la rendición de cuentas, principios que también constituyen el eje central de los Objetivos de Desarrollo Sostenible y los Principios Rectores sobre las Empresas y los Derechos Humanos. Además, a las tecnologías de IA deben aplicárseles sistemáticamente los requisitos de legalidad, legitimidad, necesidad y proporcionalidad. Asimismo, la IA debería implantarse de modo que facilite el ejercicio efectivo de los derechos económicos, sociales y culturales garantizando que se cumplan sus elementos clave de disponibilidad, asequibilidad, accesibilidad y calidad. Las personas que sufren vulneraciones de sus derechos humanos y abusos relacionados con el uso de la IA deben tener acceso a recursos judiciales y no judiciales efectivos.

Declaración Europea del Parlamento Europeo, del Consejo y de la Comisión Europea sobre los Derechos y Principios Digitales para la Década Digital, de 2023

8. La inteligencia artificial debe ser un instrumento al servicio de las personas y su fin último debe ser aumentar el bienestar humano.

9. Toda persona debería estar empoderada para beneficiarse de las ventajas de los sistemas algorítmicos y de inteligencia artificial, especialmente a fin de tomar sus propias decisiones en el entorno digital con conocimiento de causa, así como estar protegida frente a los riesgos y daños a su salud, su seguridad y sus derechos fundamentales.

Nos comprometemos a:

a) promover sistemas de inteligencia artificial centrados en el ser humano, fiables y éticos a lo largo de todo su desarrollo, despliegue y uso, en consonancia con los valores de la UE;

b) velar por un nivel adecuado de transparencia en el uso de los algoritmos y la inteligencia artificial y por qué las personas estén informadas y capacitadas para utilizarlos cuando interactúen con ellos;

c) velar por que los sistemas algorítmicos se basen en conjuntos de datos adecuados para evitar la discriminación y permitir la supervisión humana de todos los resultados que afecten a la seguridad y los derechos fundamentales de las personas;

d) garantizar que las tecnologías como la inteligencia artificial no se utilicen para anticiparse a las decisiones de las personas en ámbitos como, por ejemplo, la salud, la educación, el empleo y la vida privada;

e) proporcionar salvaguardias y adoptar las medidas adecuadas, en particular promoviendo normas fiables, para que la inteligencia artificial y los sistemas digitales sean seguros y se utilicen en todo momento con pleno respeto de los derechos fundamentales de las personas;

f) adoptar medidas para garantizar que la investigación en inteligencia artificial respete las normas éticas más estrictas y la legislación pertinente de la UE.

LOS DIFERENTES DERECHOS HUMANOS DE LAS MUJERES QUE PUEDEN SER VULNERADOS POR LA VIOLENCIA EN LÍNEA

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

17. Un gran número de deducciones y predicciones afectan profundamente al goce del derecho a la privacidad, en particular a la autonomía de las personas y su derecho a establecer los detalles de su identidad. También plantean muchas cuestiones en relación con otros derechos, como el derecho a la libertad de pensamiento y de opinión, el derecho a la libertad de expresión y el derecho a un juicio imparcial y otros derechos conexos.

CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018

3. [T]odas las formas de discriminación, intimidación, acoso y violencia en los contextos digitales impiden a las mujeres y las niñas disfrutar plenamente de sus derechos humanos y libertades fundamentales, incluido el derecho a la libertad de opinión y expresión, el derecho a la libertad de reunión pacífica y asociación, y el derecho a la privacidad, de conformidad con las obligaciones del derecho internacional, lo que obstaculiza su participación plena, efectiva y en condiciones de igualdad en los asuntos económicos, sociales, culturales y políticos y es un impedimento para lograr la igualdad de género y el empoderamiento de todas las mujeres y las niñas.

4. [E]l derecho de las mujeres y las niñas a disfrutar del más alto nivel posible de salud física y mental incluye el acceso a la información, la educación y los medios para ejercer ese derecho, tanto en el entorno virtual como fuera de él.

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

Entre algunos de los derechos humanos de las mujeres que esta violencia afecta se encuentran: el derecho a una vida libre de violencia (artículo 3 de la Convención de Belém do Pará); el derecho al respeto de la integridad física, psíquica y moral (art. 4.b de la Convención de Belém do Pará y art. 5 de la Convención Americana sobre Derechos Humanos-CADH); el derecho a la libertad y a la seguridad personales (art. 4.c de la Convención de Belém do Pará); el derecho a que se respete la dignidad inherente a la persona y que se proteja a su familia (art. 4.e de la Convención de Belém do Pará y art. 17 de la CADH); el derecho a la igualdad y no discriminación (art. 4.f de la Convención de Belém do Pará y artículo 24 de la CADH); el derecho a la libertad de expresión (artículo 13 de la CADH); el derecho a la libertad de reunión y asociación (art. 4.h de la Convención de Belém do Pará y artículos 15 y 16 de la CADH); el derecho a la privacidad (incluyendo a la protección de datos personales); el derecho a la protección de la honra y la dignidad (art. 11 de la CADH), y los derechos sexuales y reproductivos de las mujeres y las niñas. (Págs. 14-15)

LOS DIFERENTES DERECHOS HUMANOS DE LAS MUJERES QUE PUEDEN SER VULNERADOS POR LA VIOLENCIA EN LÍNEA

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2022

(Considerando 3) La violencia contra las mujeres y la violencia doméstica suponen una violación de los derechos fundamentales, como el derecho a la dignidad humana, el derecho a la vida y a la integridad de la persona, la prohibición de las penas o los tratos inhumanos o degradantes, el derecho al respeto de la vida privada y familiar, el derecho a la libertad y a la seguridad, el derecho a la protección de los datos de carácter personal, el derecho a la no discriminación, también por razón de sexo, y los derechos del menor, consagrados en la Carta y en la Convención de las Naciones Unidas sobre los Derechos del Niño.

ACNUDH, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", de 24 de junio de 2020

33. El no establecimiento de salvaguardias eficaces el uso de la tecnología de reconocimiento facial para identificar a las personas durante una reunión surte unos efectos considerablemente lesivos para los derechos a la privacidad, la libertad de expresión y la reunión pacífica. La imagen de una persona constituye uno de los atributos fundamentales de su personalidad, ya que revela características únicas que la distinguen de otras. El hecho de grabar, analizar y conservar las imágenes faciales de alguien sin su consentimiento constituye una injerencia en el ejercido el derecho a la vida privada. Al desplegar la tecnología de reconocimiento facial en las reuniones y manifestaciones, la injerencia adquiere una escala enorme e indiscriminada, ya que se requiere la recopilación y el procesamiento de imágenes faciales de todas las personas captadas por una cámara equipada con un sistema de tecnología de reconocimiento facial o conectada a un sistema de este tipo.

EL DERECHO A LA IGUALDAD Y A LA NO DISCRIMINACIÓN

CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018

[L]a violencia contra las mujeres y las niñas constituye una manifestación de la desigualdad de género y la discriminación que sufren las mujeres y las niñas, y puede obstaculizar su independencia económica e imponer costos directos e indirectos, a corto y largo plazo, a la sociedad y a las personas, incluidos, según proceda, la pérdida de medios de subsistencia y la falta de acceso a los servicios financieros digitales, y los efectos psicológicos y físicos que conlleva, así como los gastos relacionados con la atención de la salud, el sector jurídico, el bienestar social y los servicios especializados. (Pág. 3)

(En el mismo sentido: OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022, pág. 75; Declaración Europea del Parlamento Europeo, del Consejo y de la Comisión Europea sobre los Derechos y Principios Digitales para la Década Digital, de 2023, art. 13)

LOS ACTOS DE VIOLENCIA CONTRA LAS MUJERES POR RAZÓN DE GÉNERO SON TAMBIÉN DISCRIMINACIÓN

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

B. Considerando que la violencia contra las mujeres y las niñas y otras formas de violencia de género están muy extendidas en la Unión y deben entenderse como una forma extrema de discriminación que afecta gravemente a las víctimas y sus familias y comunidades, y como una violación de los derechos humanos arraigada en la desigualdad de género, que contribuyen a perpetuar y reforzar; [...]

DISCRIMINACIÓN MULTIPLE E INTERSECCIONAL

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, Informe de 18 de junio de 2018

28. Las mujeres son afectadas de forma desproporcionada por la violencia en línea y sufren consecuencias extremadamente graves a causa de ello. Su acceso a la tecnología también se ve afectado por formas interseccionales de discriminación basadas en un conjunto de otros factores, como la raza, el origen étnico, la casta, la orientación sexual, la identidad y expresión de género, la capacidad, la edad, la clase social, los ingresos, la cultura, la religión y el entorno urbano o rural. Estas formas de discriminación interseccional no solo son el resultado de una sola característica determinada, sino de la interrelación entre ellas, que puede dar lugar a consecuencias más graves. Las mujeres que se definen de formas múltiples suelen ser destinatarias de ataques en línea sobre la base de una combinación de estos factores, como la discriminación racial y el discurso de odio. Algunos grupos de mujeres, como las defensoras de los derechos humanos, las mujeres que participan en actividades políticas, como las parlamentarias, las periodistas, las blogueras, las mujeres jóvenes, las mujeres pertenecientes a minorías étnicas y las mujeres indígenas, las mujeres lesbianas, bisexuales y transgénero, las mujeres con discapacidad y las mujeres de grupos marginados, son especialmente objeto de violencia facilitada por las TIC.

(En el mismo sentido: CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018, pág. 3)

Plataforma EDVAW, Informe "La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW", de noviembre de 2022

La exposición de las mujeres a formas múltiples e interrelacionadas de discriminación también hace más probable la violencia en línea y facilitada por la tecnología, o que sus consecuencias sean más graves. La discriminación interseccional por motivos de identidad de género, expresión de género, orientación sexual, discapacidad, raza, etnia, condición indígena, edad, religión,

DISCRIMINACIÓN MULTIPLE E INTERSECCIONAL

participación en la vida pública y otros factores agravan, aumentan y complican las experiencias de violencia de género. Los estudios han revelado que las mujeres negras tienen un 84 % más de probabilidades que las mujeres blancas de ser mencionadas en tweets abusivos (Amnistía Internacional, 2018). Otro estudio encontró que el 42 % de las niñas y mujeres jóvenes que se autoidentifican como lesbianas, gays, bisexuales, transgénero, intersexuales y queer (LGBTIQ), el 14 % de las que se autoidentifican con una discapacidad y el 37 % de las que se identifican a sí mismas como pertenecientes a una minoría étnica, comunicaron haber experimentado acoso en línea relacionado con estas características (Plan International, 2020). (Pág. 10)

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 8 de marzo de 2024

(Considerando 6) La violencia contra las mujeres y la violencia doméstica pueden agravarse cuando convergen con discriminación por razón de sexo combinada con discriminación por cualquier otro motivo o motivos del artículo 21 de la Carta, en concreto la raza, el color, el origen étnico o social, las características genéticas, la lengua, la religión o el credo, las opiniones políticas o de cualquier otro tipo, la pertenencia a una minoría nacional, el patrimonio, el nacimiento, la discapacidad, la edad o la orientación sexual («discriminación interseccional»). [...]

(Considerando 71) Las víctimas que sufren discriminación interseccional corren un mayor riesgo de sufrir violencia. Podrían incluir mujeres con discapacidad, mujeres con estatuto de residencia como persona a cargo o con permiso de residencia como persona a cargo, mujeres migrantes indocumentadas, mujeres solicitantes de protección internacional, mujeres que huyen de conflictos armados, mujeres sin hogar, mujeres de origen racial o étnico minoritario, mujeres que viven en zonas rurales, mujeres que ejercen la prostitución, mujeres con bajos ingresos, mujeres detenidas, personas lesbianas, gais, bisexuales, transgénero o intersexuales, mujeres de edad avanzada o mujeres con trastornos relacionados con el consumo de alcohol y drogas. Por consiguiente, las víctimas que sufren discriminación interseccional deben recibir protección y apoyo especiales.

(En el mismo sentido: artículo 33).

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

31. Subraya que la ciberviolencia de género tiene consecuencias psicológicas, sociales y económicas negativas para las vidas de las mujeres y las niñas tanto en línea como fuera de línea; señala que la ciberviolencia de género afecta a las mujeres y las niñas de diferentes maneras como consecuencia de formas de discriminación que se solapan entre sí basadas en, además de su género, su orientación sexual, edad, raza, religión o discapacidad, entre otras cosas, y recuerda que adoptar un enfoque interseccional es fundamental para comprender estas formas específicas de discriminación;

(En el mismo sentido: párrs. D y 7).

EL DERECHO A LA INTEGRIDAD FÍSICA Y PSICOLÓGICA

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

48. Los actos de ciberviolencia, ciberacoso y suplantación dolosa se han clasificado como formas de violencia contra mujeres y [niñas y] niños capaces de socavar su integridad física y psicológica en vista de su vulnerabilidad. La Corte ha señalado recientemente que "el ciberacoso se reconoce actualmente como un aspecto de la violencia contra las mujeres y las niñas y puede adoptar una variedad de formas, como las ciberagresiones de la vida privada ... y la toma, intercambio y manejo de información y imágenes, incluidas las íntimas". En el contexto de la violencia doméstica, las parejas íntimas son con frecuencia los probables perpetradores de los actos de acoso o vigilancia cibernética.

INTERNET Y LA LIBERTAD DE EXPRESIÓN

TEDH, Caso Yildirim c. Turquía, Sentencia de 18 de marzo de 2013

54. Internet es en la actualidad el principal medio de la gente para ejercer su derecho a la libertad de expresión y de información: se encuentran herramientas esenciales de participación en actividades y debates relativos a cuestiones políticas o de interés público.

EL DERECHO A LA LIBERTAD DE EXPRESIÓN NO ES UN DERECHO ABSOLUTO

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, Informe de 18 de junio de 2018

52. [L]a libertad de expresión no es un derecho absoluto, ya que no puede invocarse para justificar términos u otras formas de expresión que constituyan incitación a la discriminación, la hostilidad o la violencia (Pacto Internacional de Derechos Civiles y Políticos, art. 20, párr. 2), incluida la violencia en línea contra la mujer.

TEDH, Caso K.U. vs. Finlandia, Sentencia de 2 de marzo de 2009

49. [...] Si bien la libertad de expresión y la confidencialidad de las comunicaciones son consideraciones primordiales y los usuarios de los servicios de telecomunicaciones e Internet deben tener una garantía de que se respetará su propia privacidad y libertad de expresión, dicha garantía no puede ser absoluta y debe ceder en ocasiones a otros imperativos legítimos, como como la prevención del desorden o el delito o la protección de los derechos y libertades de los demás. [...]

EL DERECHO A LA LIBERTAD DE EXPRESIÓN NO ES UN DERECHO ABSOLUTO

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, Informe de 18 de junio de 2018

29. La violencia en línea contra la mujer no solo viola el derecho de la mujer a llevar una vida libre de violencia y a participar en línea, sino que también socava el ejercicio democrático y la buena gobernanza y, por lo tanto, crea un déficit democrático.

73. [...] Las investigaciones indican que las respuestas inadecuadas y deficientes de los intermediarios sobre violencia en línea por razón de género pueden tener un efecto negativo en la libertad de expresión, lo que da lugar a la censura por las plataformas, la autocensura o la censura por otros usuarios, y no proporciona a las víctimas de acoso ninguna forma de reparación.

EL DERECHO A LA VIDA PRIVADA

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

50. No hay controversia sobre la aplicabilidad del artículo 8 en el presente caso: la Corte ha encontrado en la primera sentencia que la publicación de las fotografías íntimas de la demandante "atentaba contra su dignidad, transmitiendo un mensaje de humillación y falta de respeto". La publicación no consensuada de sus fotografías íntimas, la creación de perfiles falsos en las redes sociales que pretendían hacerse pasar por ella y su rastreo con el uso de un dispositivo GPS interfirieron con su disfrute de su vida privada, lo que la hizo sentir ansiedad, angustia e inseguridad. [...]

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, Informe de 18 de junio de 2018

57. El derecho a la vida privada, amparado en el artículo 12 de la Declaración Universal de Derechos Humanos y en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, se ha visto amenazado en el entorno digital. Las normas de protección de datos también se han visto amenazadas por las innovaciones en materia de TIC que han aumentado la capacidad de los Estados y de los agentes no estatales para realizar actividades de vigilancia, descifrado y recopilación y utilización masiva de datos, lo que tiene repercusiones en los derechos de las personas a la vida privada. Muchas formas de violencia en línea constituyen en sí mismas actos de violencia por razón de género que vulneran los derechos de las mujeres y las niñas a la vida privada [...]

58. En un informe reciente, el Relator Especial sobre el derecho a la privacidad subrayó la necesidad de examinar la ciberviolencia contra los más vulnerables, incluida la violencia doméstica facilitada por dispositivos digitales, los riesgos a la privacidad de los niños y los prejuicios por razón de género y otros incorporados en algoritmos.

EL DERECHO A LA VIDA PRIVADA

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

7. El derecho a la privacidad es una expresión de la dignidad humana y está vinculado a la protección de la autonomía y la identidad personales. Entre los aspectos de la privacidad que revisten especial importancia en el contexto del uso de la IA está la privacidad de la información, a saber, la información que existe o puede obtenerse sobre una persona y su vida, así como las decisiones basadas en esa información, y la libertad de adoptar decisiones en lo que respecta a la propia identidad.

14. Además de exponer la vida privada de las personas a las empresas y los Estados, estos conjuntos de datos hacen a las personas vulnerables en diversos aspectos. Las filtraciones de datos han expuesto en reiteradas ocasiones información delicada de millones de personas. Los grandes conjuntos de datos permiten innumerables formas de análisis e intercambio de datos con terceros, lo que a menudo conlleva otras intromisiones en la privacidad con consecuencias negativas para los derechos humanos. Los acuerdos que permiten a los organismos gubernamentales tener acceso directo a esos conjuntos de datos en poder de las empresas, por ejemplo, aumentan la probabilidad de que se produzcan injerencias arbitrarias o ilegales en el derecho a la privacidad de las personas afectadas. [...]

15. Cabe señalar que los sistemas de IA no se basan exclusivamente en el tratamiento de datos de carácter personal. No obstante, aunque los datos no sean personales, su uso puede tener consecuencias negativas para los derechos humanos, incluido el derecho a la privacidad [...].

(En el mismo sentido: Declaración Europea del Parlamento Europeo, del Consejo y de la Comisión Europea sobre los Derechos y Principios Digitales para la Década Digital, de 2023, art. 12)

LAS RESTRICCIONES AL DERECHO A LA PRIVACIDAD Y LA LEGALIDAD Y PROPORCIONALIDAD DE LAS MISMAS

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

39. [L]as restricciones del derecho a la privacidad deben estar previstas en la ley y ser necesarias y proporcionadas para alcanzar un objetivo legítimo. En la práctica, eso significa que los Estados tienen que valorar detenidamente si una medida podrá alcanzar un objetivo establecido, hasta qué punto es importante ese objetivo y qué efectos tendrá esa medida. Los Estados también deben determinar si podrían lograr los mismos resultados con la misma eficacia aplicando enfoques menos invasivos y, en caso afirmativo, deberían adoptar esas medidas. La Alta Comisionada ya ha señalado la necesidad de esos límites y garantías en el contexto de la vigilancia por parte de los organismos de inteligencia y las fuerzas del orden. Cabe señalar que las pruebas de necesidad y proporcionalidad también pueden llevar a la conclusión de que no deben adoptarse determinadas medidas. Por ejemplo, los requisitos de conservación general e indiscriminada de datos de comunicaciones impuestos a las empresas de telecomunicaciones y de otros sectores no pasarían la prueba de proporcionalidad. Del mismo modo, sería desproporcionado imponer requisitos de identificación biométrica a los beneficiarios de la asistencia social sin ofrecerles una alternativa. Además, es fundamental que estas medidas no se evalúen de forma aislada, sino que se tengan debidamente en cuenta los efectos acumulativos de medidas distintas que interactúan. Por ejemplo, antes de decidir implantar nuevas herramientas de vigilancia basadas en la IA, un Estado debe hacer balance de las capacidades ya existentes y de sus efectos en el disfrute del derecho a la privacidad y otros derechos.

EL ANONIMATO Y EL PSEUDO-ANONIMATO COMO ASPECTOS FUNDAMENTALES PARA EL EJERCICIO DE LOS DERECHOS A LA VIDA PRIVADA Y A LA LIBERTAD DE EXPRESIÓN LAS MUJERES

CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018

6. [E]l cifrado y el anonimato pueden contribuir al pleno disfrute de los derechos humanos de las personas, incluido el derecho a la libertad de opinión y de expresión y el derecho a la privacidad, de conformidad con el derecho internacional, y pueden empoderar a las personas, incluidas las mujeres y las niñas, para acceder a la información y las ideas, pedir ayuda, asistencia y asesoramiento y explorar y expresar ideas libremente en relación con su identidad y sus derechos humanos.

(En el mismo sentido: ACNUDH, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", de 24 de junio de 2020, párr. 25)

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, Informe de 18 de junio de 2018

75. [...] Si bien los acosadores pueden ocultarse tras el velo del anonimato que hace más difícil su identificación y la adopción de medidas contra ellos, el anonimato y el pseudoanonimato también son aspectos fundamentales de la vida privada y la libertad de expresión de las mujeres. Las mujeres que tienen perfiles en línea anónimos o pseudoanónimos también sufren consecuencias adversas a causa de las políticas de anonimato de ciertos intermediarios. Desde una perspectiva de género, las mujeres deberían estar en condiciones de utilizar seudónimos, que podrían ayudarlas a huir de una pareja que las maltrata, de acosadores o de acosadores reincidentes, y a desvincularse de cuentas relacionadas con la publicación de pornografía no consentida. Como resultado de ello, las mujeres, especialmente las defensoras de los derechos humanos, que prefieren permanecer en el anonimato en sitios web como Facebook, suelen ser denunciadas por los acosadores por poseer un perfil "falso". En lugar de entablar acciones contra los acosadores, algunas veces los intermediarios exigen a las mujeres afectadas que revelen su identidad, lo que puede ponerlas en riesgo de sufrir daños graves. Por esta razón, la política ha sido objeto de fuertes críticas por parte de algunos grupos de la sociedad civil. [...] En este contexto, las salvaguardias de los derechos humanos contra la censura arbitraria por los intermediarios son fundamentales.

EL DERECHO A LA ELIMINACIÓN DEL MATERIAL ILÍCITAMENTE CREADO/OBTENIDO Y PUBLICADO

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

(Considerando 86) A fin de garantizar que las víctimas de los delitos de ciberviolencia establecidos en la presente Directiva puedan ejercer eficazmente su derecho a la eliminación del material ilícito relacionado con esos delitos, los Estados miembros deben fomentar la cooperación en materia de autorregulación entre los prestadores de servicios intermediarios pertinentes. Para garantizar que dicho material se detecte pronto, que se actúe contra él eficazmente y que las víctimas de esos delitos reciban la asistencia y el apoyo adecuados, los Estados miembros deben facilitar también el establecimiento de medidas de autorregulación de carácter voluntario o dar a conocer las existentes, como códigos de conducta. Dicha facilitación debe incluir medidas de autorregulación para la detección de riesgos sistemáticos, en particular para reforzar mecanismos destinados a combatir la ciberviolencia y mejorar la formación de los empleados de los prestadores de servicios intermediarios encargados de la prevención de la violencia y la prestación de asistencia y apoyo a las víctimas. . [E]l cifrado y el anonimato pueden contribuir al pleno disfrute de los derechos humanos de las personas, incluido el derecho a la libertad de opinión y de expresión y el derecho a la privacidad, de conformidad con el derecho internacional, y pueden empoderar a las personas, incluidas las mujeres y las niñas, para acceder a la información y las ideas, pedir ayuda, asistencia y asesoramiento y explorar y expresar ideas libremente en relación con su identidad y sus derechos humanos. [...]

EL DERECHO ASOCIACIÓN Y DE REUNIÓN Y SU POSIBLE AFECTACIÓN POR EL USO DE LAS TIC CON FINES DE VIGILANCIA POR PARTE DE LAS AUTORIDADES

ACNUDH, Informe "Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas", de 24 de junio de 2020

4. El derecho de reunión pacífica desempeña un papel importante en la movilización de la población, pues permite formular y expresar agravios y aspiraciones y facilita celebrar actos y, aún más importante, influir en las políticas públicas. [...] Las nuevas tecnologías han desempeñado un papel en muchas de estas protestas, ya sea como medio para posibilitar la organización y la coordinación o como herramienta para restringir o vulnerar los derechos humanos de los manifestantes.

5. El derecho de reunión pacífica incluye el derecho a celebrar encuentros, sentadas, huelgas, mítines, eventos o manifestaciones multitudinarias, tanto en Internet como fuera de esta red. Constituye un medio para el ejercicio de muchos otros derechos amparados por el derecho internacional, con los que está intrínsecamente vinculado y con los que sientan las bases para la participación en protestas pacíficas, en particular los derechos a la libertad de expresión y a participar en la dirección de los asuntos públicos. Estos derechos están enunciados en la Declaración Universal de Derechos Humanos (art. 20, párr. 1), el Pacto Internacional de Derechos Civiles y Políticos (art. 21) y la Convención sobre los Derechos del Niño (art. 15). Otros instrumentos pertinentes en la materia son la Declaración sobre el Derecho y el Deber de los Individuos, los Grupos y las Instituciones de Promover y Proteger los Derechos Humanos y las Libertades Fundamentales Universalmente Reconocidos (Declaración sobre los Defensores de los Derechos Humanos), en la que también se establecen reglas y principios normativos aplicables, y, a nivel regional, varias directrices sobre la aplicación del derecho de reunión pacífica.

(En el mismo sentido: Declaración Europea del Parlamento Europeo, del Consejo y de la Comisión Europea sobre los Derechos y Principios Digitales para la Década Digital, de 2023, art. 13)

35. Las técnicas de grabación audiovisual y de reconocimiento facial solo deben utilizarse cuando dichas medidas cumplan la triple condición de la legalidad, la necesidad y la proporcionalidad. Se ha cuestionado la posibilidad de que el recurso a la tecnología de reconocimiento facial durante las protestas pacíficas pueda cumplir con los requisitos de necesidad y proporcionalidad, dada su invasividad y sus graves efectos de desistimiento del ejercicio de un derecho. Las autoridades deben abstenerse como principio general de grabar a los asistentes a reuniones. Dada la necesidad de respetar el imperativo de proporcionalidad, las excepciones solo pueden contemplarse cuando haya indicios concretos de que se están cometiendo realmente delitos graves o haya motivos para sospechar la inminencia de un comportamiento delictivo grave, como la violencia o el uso de armas de fuego. Las grabaciones existentes solo deben utilizarse para la identificación de asistentes a una reunión que sean sospechosos de delitos graves.

EL DERECHO ASOCIACIÓN Y DE REUNIÓN Y SU POSIBLE AFECTACIÓN POR EL USO DE LAS TIC CON FINES DE VIGILANCIA POR PARTE DE LAS AUTORIDADES

36. Si bien se desaconseja el uso de la tecnología de reconocimiento facial en el caso de las reuniones pacíficas, los gobiernos que aún sigan utilizando esta tecnología deben asegurarse de que lo hacen fundamentándose en una base jurídica clara, en particular un marco regulador sólido y respetuoso de los derechos humanos. Además, las autoridades que continúen utilizando técnicas de grabación audiovisual y reconocimiento facial deberían implantar un marco regulador con disposiciones que protejan eficazmente los datos personales, en particular tratándose de imágenes faciales y los datos derivados de ellos. Las medidas deben preceptuar el borrado inmediato de todos los datos, salvo los segmentos específicos que puedan ser necesarios para llevar a cabo una investigación penal y el enjuiciamiento de delitos violentos. Todas las personas afectadas deben tener el derecho a acceder y solicitar la rectificación y eliminación de toda información almacenada sin un propósito legítimo y sin fundamento jurídico, salvo cuando esta operación pueda impedir el desarrollo de una investigación o la incoación de un procedimiento penal en que esos datos sean necesarios.

37. Además, todo uso de la tecnología de grabación audiovisual y de reconocimiento facial debe estar sujeto a mecanismos de supervisión bien estructurados y dotados de recursos. Si bien parte de la supervisión puede estar a cargo de autoridades independientes e imparciales de protección de datos, los Estados deberían considerar la posibilidad de adoptar medidas adicionales, en particular la participación de un órgano independiente, preferiblemente de carácter judicial, encargado de autorizar el uso de medidas de tecnología de reconocimiento facial en una reunión. Sea como fuere, todo uso de la tecnología de grabación y reconocimiento facial debe poder ser objeto de impugnación judicial. En todas las circunstancias, las autoridades deben ser transparentes en cuanto al uso de la tecnología de grabación y reconocimiento facial y notificar siempre a los ciudadanos cuándo están siendo grabados y puedan ser grabados y/o que sus imágenes podrían ser procesadas en un sistema de reconocimiento facial.

EL DERECHO A LA PARTICIPACIÓN POLÍTICA

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém do Pará, de 2022

Cabe señalar que el efecto silenciador de la violencia de género en línea no solo repercute en el desarrollo personal de las mujeres, sino que además socava la dimensión social del derecho a la libertad de expresión relacionada con la libre deliberación democrática y el buen gobierno, puesto que la sociedad deja de contar con la diversidad de voces de las mujeres. De acuerdo con la REVM-ONU, "además de los efectos en las personas, una grave consecuencia de la violencia de género en línea y facilitada por las TIC es una sociedad en que las mujeres ya no se sienten seguras en línea o fuera de línea, debido a la impunidad generalizada de los autores de la violencia de género. La violencia en línea contra la mujer no solo viola el derecho de la mujer a llevar una vida libre de violencia y a participar en línea, sino que también socava el ejercicio democrático y la buena gobernanza y, por lo tanto, crea un déficit democrático". (Pág. 98)

EL DERECHO A LA PARTICIPACIÓN POLÍTICA

CDH, Grupo de Trabajo sobre la cuestión de la discriminación contra las mujeres y las niñas, Informe "Activismo de las niñas y las jóvenes", de 10 de mayo de 2022

39. La violencia de género y el acoso digitales añaden una capa más de obstáculos al activismo de las niñas y las jóvenes. Las tecnologías digitales pueden utilizarse para chantajear, controlar, vigilar, coaccionar, acosar, humillar o cosificar a las niñas y jóvenes activistas, hasta el punto de recurrir a contenido pornográfico "ultrafalso" y a amenazas de muerte. Como consecuencia, muchas víctimas de estas prácticas limitan sus actividades en línea, lo que las lleva a autocensurarse, a soportar el estigma en sus familias y comunidades, o a huir por completo de los espacios digitales. La mayoría de las jóvenes y niñas consultadas habían sufrido algún tipo de ciberabuso directo y de género, como mensajes amenazantes, acoso sexual e intercambio de imágenes privadas sin su consentimiento. Los ataques contra las niñas y jóvenes activistas suelen organizarse con el objetivo de desacreditarlas, deslegitimarlas y exponerlas al ridículo, al desprecio o a la difamación. En algunos casos, sus familias pueden prohibirles continuar con su activismo por el daño a la reputación que puede suponer. En algunos países, la sola presencia de niñas y jóvenes en los medios sociales llega a constituir un gran riesgo para su integridad personal. La recopilación de datos a gran escala y los análisis basados en algoritmos que tienen como objetivo la información sensible crean nuevas amenazas para las activistas, especialmente para aquellas pertenecientes a comunidades de personas lesbianas, gais, bisexuales, transgénero, intersexuales y queer. Como explicó una activista: "al hacer campañas en Internet, a veces tememos hablar abiertamente porque sabemos que existe una vigilancia digital por parte del Gobierno".

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

34. Lamenta que la ciberviolencia de género sea cada vez más común y reduzca la participación de las mujeres y las personas LGBTIQ en la vida y el debate públicos, lo que erosiona la democracia de la Unión y sus principios e impide a las mujeres y personas LGBTIQ disfrutar plenamente de sus derechos y libertades fundamentales, en particular de la libertad de expresión; lamenta asimismo que la ciberviolencia de género también dé lugar a censura; lamenta que ese «efecto silenciador» se haya dirigido especialmente contra mujeres activistas, incluidas mujeres y chicas feministas, activistas LGBTIQ+, artistas, mujeres en sectores dominados por los hombres, periodistas, políticas, defensoras de los derechos humanos y blogueras, disuadiendo a las mujeres de participar en la vida pública, incluidos los ámbitos de la política y la toma de decisiones; expresa su preocupación por el hecho de que el efecto amedrentador de la ciberviolencia de género a menudo se extienda a la realidad fuera de línea y por que la normalización de la violencia en línea contra las mujeres que participan en el debate público contribuya activamente al bajo porcentaje de denuncia de estos delitos y limite la participación de las mujeres jóvenes en particular;

(En el mismo sentido: Declaración Europea del Parlamento Europeo, del Consejo y de la Comisión Europea sobre los Derechos y Principios Digitales para la Década Digital, de 2023, art. 12).

EL DERECHO DE ACCESO A LA INFORMACIÓN COMO PARTE DEL DERECHO A LA LIBERTAD DE EXPRESIÓN Y DEL DERECHO DE PARTICIPACIÓN POLÍTICA DE LAS MUJERES

CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018

7. [A] fin de asegurar la plena participación de las mujeres y las niñas en la era digital, es necesario abordar la cuestión de la brecha digital, que afecta de manera desproporcionada a las mujeres y las niñas que viven en zonas rurales o alejadas, facilitando a las mujeres y las niñas igual acceso a las tecnologías digitales, a la educación en ciencia, tecnología, ingeniería y matemáticas y a un entorno tecnológico que propicie la participación de todas las mujeres y las niñas, entre otras cosas, mediante el uso de tecnologías de apoyo, así como promover un entorno digital seguro para las mujeres y las niñas, sin discriminación ni riesgo de violencia y prestando especial atención a las necesidades de las mujeres y las niñas que se enfrentan a desigualdades sistémicas interrelacionadas.

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, Informe de 18 de junio de 2018

53. El acceso a la información incluye el acceso a las TIC, que suele caracterizarse por la desigualdad entre los géneros o una brecha digital de género, a saber, la discriminación por razón de género contra la mujer en el acceso y el uso de las TIC, que obstaculiza el pleno disfrute por la mujer de sus derechos humanos. El acceso de las mujeres a las TIC es parte de su derecho a la libertad de expresión, y es necesario para el disfrute de otros derechos humanos fundamentales, como los derechos a participar en la adopción de decisiones políticas y a la no discriminación.

(En el mismo sentido: Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia, párr. 38).

EL DERECHO DE ACCESO A LA JUSTICIA

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, Informe de 18 de junio de 2018

77. Si bien es esencial mantener el anonimato de los usuarios, la identificación de los autores es necesaria si ha de abordarse la violencia en línea por razón de género. El acceso a justicia requiere procesos de identificación y la capacidad de vincular los identificadores digitales, como una dirección IP, con los dispositivos y los autores materiales, por un poder judicial independiente. Un conjunto de instrumentos jurídicos cuidadosamente adaptados a este fin podría facilitar el proceso de identificación.

Comité CEDAW, Recomendación general nº 33 sobre el acceso de las mujeres a la justicia, de 3 de agosto de 2015

16. [...] d) Garanticen el acceso a la Internet y otras tecnologías de la información y las comunicaciones para mejorar el acceso de la mujer a los sistemas de justicia a todos los niveles, y presten atención al desarrollo de una infraestructura interna, incluidas las videoconferencias, para facilitar la celebración de audiencias y compartir, reunir y apoyar datos e información entre los interesados directos; [...]

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

2. Recuerda que no hay definición común de ciberviolencia de género, lo que genera diferencias considerables en la medida en que los Estados miembros la previenen y combaten, y provoca grandes disparidades entre los Estados miembros en cuanto a la protección, el apoyo y la compensación para las víctimas; pide, por tanto, a la Comisión y a los Estados miembros que definan y adopten una definición común de ciberviolencia de género que facilite la labor de análisis de las distintas formas de ciberviolencia de género y la lucha contra ella, garantizando así que las víctimas de la ciberviolencia de género en los Estados miembros tengan un acceso efectivo a la justicia y a servicios de apoyo especializados;

(En el mismo sentido: párr. 43).

EL DERECHO DE ACCESO A LA JUSTICIA

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, Informe de 18 de junio de 2018

97. Los Estados también deben promover la alfabetización digital en el uso de Internet y las TIC para todos, sin discriminación por razón de sexo o género, y promover la igualdad de género en todos los niveles de la educación, incluida la educación en línea, desde la primera infancia.

(En el mismo sentido: Comisión Africana de Derechos Humanos y de los Pueblos, Resolución sobre la protección de las mujeres contra la violencia digital en África - ACHPR/Res. 522 (LXXII), de 11 de agosto de 2022; Declaración Europea del Parlamento Europeo, del Consejo y de la Comisión Europea sobre los Derechos y Principios Digitales para la Década Digital, de 2023, párr. 4.a).

Relator Especial sobre el derecho a la privacidad, Informe de 24 de marzo de 2020

43. Los Estados y los agentes no estatales deberían contrarrestar la violencia de género mediante formas de abuso basadas en el género que invadían la privacidad y eran facilitadas por la tecnología:

a) Impartiendo educación, divulgación y capacitación con perspectiva de género a los usuarios de Internet sobre la violencia en línea en las escuelas y comunidades; [...]

Comité CEDAW, Recomendación general nº 36 sobre el derecho de las niñas y las mujeres a la educación, de 27 de noviembre de 2017

61. Un campo técnico y profesional básico en el que las niñas y las mujeres están infrarrepresentadas es el de la tecnología de la información y las comunicaciones. Al 60% de la población mundial, en su mayoría niñas y mujeres, se le niega el derecho a beneficiarse del poder transformador de Internet. Si se quiere superar la brecha digital entre los hombres y las mujeres en el uso de las nuevas tecnologías y proporcionar a las mujeres igualdad de acceso a la información y las oportunidades de empleo en esos sectores, los centros de enseñanza deben eliminar los obstáculos que dan lugar a su exclusión.

(En el mismo sentido: CDH, Grupo de Trabajo sobre la cuestión de la discriminación contra las mujeres y las niñas, Informe "Activismo de las niñas y las jóvenes", de 10 de mayo de 2022, parr. 59).

EL DERECHO AL TRABAJO

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

J. Considerando que la conectividad a internet y el acceso a la esfera pública digital son cada vez más necesarios para el desarrollo de nuestras sociedades y economías; que el empleo implica un uso cada vez mayor de las soluciones digitales y es cada vez más dependiente de dichas soluciones, lo que da lugar a un mayor riesgo de que las mujeres sufran ciberviolencia de género al participar en el mercado laboral y en actividades económicas;

29. [...] subraya que la ciberviolencia de género también puede tener repercusiones económicas negativas como una menor presencia en el trabajo, el riesgo de pérdida del empleo, una mayor dificultad a la hora de buscar trabajo y una menor calidad de vida, y destaca que algunas de estas repercusiones agravan otras formas de discriminación a las que se enfrentan las mujeres y las personas LGBTIQ en el mercado laboral;

LA INTERDEPENDENCIA DE LOS DERECHOS HUMANOS AFECTADOS

CIDH, Anexo 1. "Estándares y recomendaciones. Violencia y discriminación contra mujeres, niñas y adolescentes", de 14 noviembre de 2019

2. El derecho de las mujeres a una vida libre de violencia es indivisible e interdependiente respecto de otros derechos humanos, como los derechos a la vida, la salud, la libertad y la seguridad de la persona, la igualdad y la misma protección en el seno de la familia, la protección contra la tortura y otros tratos crueles, inhumanos o degradantes, entre otros.

2.7 Deberes de los Estados en materia de violencia en línea contra las mujeres

A) El deber de diligencia debida.

NO CONTAR CON UN PROCEDIMIENTO ADECUADO VULNERA EL DEBER A LA DEBIDA DILIGENCIA

TEDH, Caso K.U. vs. Finlandia, Sentencia de 2 de marzo de 2009

48. [...] El Tribunal señala al mismo tiempo que el incidente en cuestión tuvo lugar en 1999, es decir, en un momento en que era bien sabido que Internet, precisamente por su carácter anónimo, podía utilizarse con fines delictivos [...]. Además, durante el decenio anterior se había conocido ampliamente el problema generalizado del abuso sexual de niños. Por lo tanto, no se puede decir que el gobierno demandado no haya tenido la oportunidad de implementar un sistema para proteger a los niños víctimas de ser expuestos como objetivos de enfoques pedofilos a través de Internet.

EL DEBER REFORZADO DE DEBIDA DILIGENCIA EN EL MARCO DE LA VIOLENCIA EN LÍNEA

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, Informe de 18 de junio de 2018

62. Los Estados tienen la obligación de derechos humanos de garantizar que tanto los agentes estatales como los no estatales se abstengan de incurrir en todo acto de discriminación o violencia contra la mujer. Los Estados tienen una responsabilidad directa con respecto a la violencia perpetrada por los agentes del propio Estado. También tienen obligaciones de diligencia debida a fin de prevenir, investigar y castigar los actos de violencia contra la mujer cometidos por empresas privadas, como los intermediarios de Internet, de conformidad con el artículo 2 e) de la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer. El artículo 4 c) de la Declaración sobre la Eliminación de la Violencia contra la Mujer insta a los Estados a proceder con la debida diligencia a fin de prevenir, investigar y castigar todo acto de violencia contra la mujer.

63. En el marco de su recomendación general núm. 35 (2017), el Comité para la Eliminación de la Discriminación contra la Mujer recomendó a los Estados que fomentaran la participación del sector privado, en particular de las empresas y las sociedades transnacionales, en los esfuerzos por erradicar todas las formas de violencia por razón de género contra la mujer y que asumieran la responsabilidad por todas las formas de violencia. De ello se desprende que debe alentarse a los medios sociales y los medios en línea a crear o fortalecer los mecanismos centrados en la erradicación de los estereotipos de género, y a poner fin a toda violencia por razón de género cometida en sus plataformas.

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

[P]or virtud del principio de debida diligencia reforzada, los Estados deben reconocer la naturaleza sistémica de la violencia en línea contra la mujer e implementar medidas integrales para atajar las causas estructurales que dan lugar a esta violencia, incluyendo la discriminación de género que la perpetúa en espacios digitales. (Pág. 115)

[E]n casos de violencia de género contra las mujeres facilitada por las TIC, las autoridades deben llevarla [la investigación] a cabo de forma seria, imparcial, efectiva, orientada a la determinación de la verdad y con una perspectiva de género. [...] (Pág. 118)

Relator Especial sobre el derecho a la privacidad, Informe de 24 de marzo de 2020

45. Los Estados y los agentes no estatales deberían:

b) Asegurar, independientemente del género, que: [...]

ii) Se adoptaran todas las medidas legislativas, administrativas, técnicas y de otra índole necesarias, de conformidad con las normas internacionales pertinentes y el derecho de los derechos humanos, en consulta con los interesados, para prevenir, reparar y eliminar el discurso de odio en línea, el acoso y la violencia relacionada con la tecnología por razón de género, y que esas iniciativas garantizaran la rendición de cuentas del sector privado;

EL DEBER REFORZADO DE DEBIDA DILIGENCIA EN EL MARCO DE LA VIOLENCIA EN LÍNEA

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 8 de marzo de 2024

(Considerando 6) [...] Por consiguiente, los Estados miembros deben prestar la debida atención a las víctimas afectadas por la discriminación interseccional, adoptando medidas específicas. Las personas afectadas por la discriminación interseccional corren un mayor riesgo de sufrir violencia de género. Por tanto, los Estados miembros deben tener en cuenta este mayor riesgo al aplicar las medidas previstas en la presente Directiva, especialmente en lo referente a la evaluación individual para determinar las necesidades de protección de las víctimas, el apoyo especializado para estas y la formación e información para los profesionales que tengan probabilidades de estar en contacto con ellas.

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, Informe de 18 de junio de 2018

19. [...] Existe un riesgo considerable de que el uso de las TIC sin aplicar un enfoque basado en los derechos humanos y la prohibición de la violencia en línea por razón de género puedan llevar a un aumento aun mayor de la discriminación sexual y por razón de género, y de la violencia contra las mujeres y las niñas en la sociedad.

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

12. Las formas digitales de violencia de género contra las mujeres pueden ser particularmente graves para las mujeres y las niñas en riesgo de sufrir o expuestas a formas interseccionales de discriminación, y pueden verse exacerbadas por factores como la discapacidad, la orientación sexual, la afiliación política, la religión y el origen social. , estatus migratorio o estatus de celebridad, entre otros. [...]

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

32. Pide a la Comisión y a los Estados miembros que presten especial atención a las formas interseccionales de ciberviolencia de género que pueden afectar a mujeres y niñas pertenecientes a grupos que se encuentran en una situación vulnerable, como las minorías étnicas, las personas con discapacidad y las personas LGBTIQ; [...]

EL DEBER DE DEBIDA DILIGENCIA Y EL ENFOQUE DE GÉNERO DE LA VIOLENCIA EN LÍNEA

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, Informe de 18 de junio de 2018

85. Aun en los casos en que existe un marco jurídico especializado, los mecanismos jurídicos y normativos, incluidos los funcionarios encargados de hacer cumplir la ley, no siempre están debidamente calificados o preparados para aplicarlo eficazmente debido a la capacitación insuficiente con perspectiva de género y la percepción general de que los abusos en línea no son un delito grave.

102. Los Estados deben aplicar una perspectiva de género a todas las formas de violencia en línea, que por lo general están tipificadas de una manera neutra en cuanto al género, a fin de considerarlas actos de violencia por razón de género. Los procedimientos de acción penal o civil deben permitir a las mujeres víctimas interponer medidas judiciales con la debida protección de su intimidad, y evitar la victimización secundaria de la mujer; sin esa protección, las víctimas que intentan suprimir contenidos podrían correr el riesgo de que su caso se hiciera aún más público.

CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018

10.b) [I]ntegración de las perspectivas de género, y aseguren la pronta, plena y eficaz participación de las mujeres y las niñas en la elaboración y aplicación de políticas, leyes, programas, proyectos, estrategias nacionales e instrumentos reglamentarios y técnicos nacionales en la esfera de las tecnologías digitales; creen mecanismos de vigilancia y rendición de cuentas para garantizar la aplicación de políticas y reglamentos que tengan en cuenta las cuestiones de género, y analicen las repercusiones de género de esas políticas en consulta y colaboración con mujeres especialistas en tecnología digital, las organizaciones de la sociedad civil y los defensores de la igualdad de género. [...]

i) Incorporen una perspectiva de género en sus sistemas de justicia penal y en las iniciativas encaminadas a prevenir y combatir la delincuencia, incluida la delincuencia organizada transnacional facilitada por la tecnología digital, en particular elaborando y aplicando leyes, políticas y programas de justicia penal nacional que tengan en cuenta la importante función y las necesidades específicas de las mujeres y las niñas y promoviendo medidas específicas de género en las políticas de prevención del delito y protección.

(En el mismo sentido: Comisión Africana de Derechos Humanos y de los Pueblos, Resolución sobre la protección de las mujeres contra la violencia digital en África - ACHPR/Res. 522 (LXXII), de 11 de agosto de 2022).

EL DEBER DE DEBIDA DILIGENCIA Y EL ENFOQUE DE

TEDH, Caso K.U. vs. Finlandia, Sentencia de 2 de marzo de 2009

46. [...] Cuando el bienestar físico y moral de un niño se ve amenazado, ese mandato adquiere una importancia aún mayor. La Corte señala a este respecto que el abuso sexual es sin duda un tipo de delito abominable, con efectos debilitantes para sus víctimas. Los niños y otras personas vulnerables tienen derecho a la protección del Estado, en forma de disuasión efectiva, contra tipos tan graves de injerencia en aspectos esenciales de su vida privada.

EL DEBER DE DEBIDA DILIGENCIA Y EL ENFOQUE DE DISCAPACIDAD EN EL MARCO DE LA VIOLENCIA EN LÍNEA

Directiva del Parlamento Europeo y del Consejo, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

(Considerando 72) Las mujeres con discapacidad sufren de manera desproporcionada violencia contra las mujeres y violencia doméstica y, debido a su discapacidad, a menudo tienen dificultades para acceder a las medidas de protección y apoyo. Por consiguiente, los Estados miembros deben garantizar que puedan disfrutar plenamente de los derechos enunciados en la presente Directiva, en igualdad de condiciones con las demás personas, y prestar la atención debida a la especial vulnerabilidad de esas víctimas y a sus probables dificultades para buscar ayuda.

Comité sobre los Derechos de las Personas con Discapacidad (CDPD), Observación general nº 8 sobre el derecho de las personas con discapacidad al trabajo y al empleo, de 7 de octubre de 2022

60. A fin de cumplir con la obligación de facilitar el derecho de las personas con discapacidad al trabajo y al empleo, los Estados partes deben adoptar medidas positivas para permitir y ayudar a estas personas a recibir enseñanza y formación técnica y profesional, e implementar planes de educación técnica y profesional para facilitar el acceso al empleo. Los Estados partes también tienen la obligación de emprender o promover la investigación y el desarrollo, y promover la disponibilidad y el uso de nuevas tecnologías, incluidas las tecnologías de la información y las comunicaciones, ayudas para la movilidad, dispositivos técnicos y tecnologías de apoyo, dando prioridad a las de precio asequible.

61. Para cumplir con la obligación de hacer efectivo el derecho de las personas con discapacidad al trabajo y al empleo, los Estados partes deben reconocer ese derecho en su sistema jurídico nacional y dotarse de una política nacional con un plan de acción detallado para su implementación. Deberían asignarse suficientes recursos a la política y el plan a fin de aumentar la participación de las personas con discapacidad, especialmente las mujeres con discapacidad, en el trabajo y el empleo. Los Estados partes también están obligados a proporcionar a las personas con discapacidad información accesible sobre las nuevas tecnologías desarrolladas en virtud de la obligación de facilitar.

EL DEBER DE DEBIDA DILIGENCIA EN EL MARCO DE LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

48. Los Estados y las empresas deben velar por que se observe de manera general la diligencia debida en materia de derechos humanos cuando se adquieran, desarrollen, implanten y exploten sistemas de IA, así como antes de que se compartan o utilicen los macrodatos que se hayan recogido sobre personas particulares. Además de financiar y dirigir estos procesos, los Estados también pueden exigir a las empresas que observen en general la diligencia debida en materia de derechos humanos, o incentivarlas de otro modo para que lo hagan.

49. Los procesos de diligencia debida en materia de derechos humanos tienen por objetivo identificar, evaluar, prevenir y mitigar los efectos adversos sobre los derechos humanos que una entidad pueda causar o a los que pueda contribuir o estar directamente vinculada. Cuando los procesos de diligencia debida revelen que un uso de la IA es incompatible con los derechos humanos, debido a la falta de medios efectivos para mitigar los daños, este tipo de uso debería abandonarse. La evaluación de los efectos sobre los derechos humanos es un elemento esencial de los procesos de diligencia debida en materia de derechos humanos. La diligencia debida debe observarse a lo largo de todo el ciclo de vida de los sistemas de IA. Debe prestarse especial atención a los efectos desproporcionados de estos sobre las mujeres y las niñas, las personas lesbianas, gais, bisexuales, transgénero y ***queer***, las personas con discapacidad, las personas pertenecientes a minorías, las personas mayores, las personas en situación de pobreza y otras personas en situación de vulnerabilidad.

Relator Especial sobre el derecho a la privacidad, Informe de 24 de marzo de 2020

45. Los Estados y los agentes no estatales deberían:

[...]

f) Proporcionar fácil acceso a los perfiles de datos y detectar los prejuicios de género mediante, por ejemplo, la auditoría algorítmica;

[...]

h) Establecer directrices sobre el desarrollo de la inteligencia artificial, incorporando el género, el derecho a la vida privada y los principios de protección de datos; [...]

EL DEBER DE LA DEBIDA DILIGENCIA Y LOS INTERMEDIARIOS

Recomendación CM/Rec(2014)6, del Consejo de Ministros del Consejo de Europa sobre una Guía de los derechos humanos para los usuarios de Internet, de 16 de abril de 2014

2. Las obligaciones de los Estados en cuanto a respetar, proteger y promover los derechos humanos incluyen la supervisión de las empresas privadas. Los derechos humanos, que son universales e indivisibles, así como las normas relacionadas, prevalecen sobre las condiciones generales impuestas a los usuarios de Internet por cualquier actor del sector privado.

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

53. Los Estados pueden reforzar la protección de los derechos humanos exigiendo sistemáticamente una conducta empresarial responsable. Por ejemplo, cuando los organismos de crédito a la exportación ofrezcan apoyo a las empresas de tecnología de IA, deben velar por que estas empresas tengan un sólido historial de conducta respetuosa con los derechos y puedan demostrarlo a través de procesos rigurosos de diligencia debida.

Relator Especial sobre el derecho a la privacidad, Informe de 24 de marzo de 2020

46. Las empresas deberían:

a) Aplicar los Principios Rectores sobre las Empresas y los Derechos Humanos y la correspondiente orientación sobre género a fin de respetar los derechos humanos de todas las personas afectadas por sus prácticas;

b) Ejercer la diligencia debida en el ámbito de los derechos humanos para determinar, prevenir, mitigar y abordar las vulneraciones de los derechos a la privacidad y la no discriminación por motivos de género, entre otras cosas mediante:

I) Evaluaciones de impacto en los derechos humanos que incorporaran los derechos a la privacidad y la no discriminación por motivos de género, al idear o modificar sus productos y servicios, e incluir consultas con organizaciones de la sociedad civil y otros expertos y corroboradas por un tercero externo acreditado y con experiencia en el ámbito de la privacidad;

II) La integración de las conclusiones de las evaluaciones de impacto:

a) Impartiendo capacitación y directrices a los gerentes, empleados y otras personas, incluidos los contratistas;

b) Adoptando políticas y procedimientos en los que se definiera cómo respondería la empresa a las limitaciones de las comunicaciones o el acceso a contenidos;

c) Estableciendo sistemas de alerta temprana en los procesos empresariales para determinar los riesgos en materia de derechos humanos y reaccionar oportunamente;

d) Privacidad;

e) Denegando las peticiones que infringían indebidamente el derecho a la Respaldando la investigación y el desarrollo de soluciones tecnológicas apropiadas para el acoso, el abuso y la misoginia en línea, entre ellas medios para descubrir e identificar cuentas y bots vinculados a los Estados;

f) Haciendo el seguimiento de problemas concretos relacionados con la privacidad y el género;

EL DEBER DE LA DEBIDA DILIGENCIA Y LOS INTERMEDIARIOS

c) Establecer códigos de conducta y condiciones de servicios para gestionar las páginas de los medios sociales que promovían la violencia de género, los estereotipos de género perjudiciales y la distribución de imágenes íntimas sin consentimiento;

d) Tomar medidas eficaces para que sus políticas y prácticas fueran transparentes, entre ellas la de aplicar condiciones de servicio y procedimientos de examen informatizados, y respetar las debidas garantías procesales; [...]

f) Instaurar mecanismos de supervisión independientes para vigilar el resultado de las decisiones de moderación de contenidos; g) Instituir, en consulta con las comunidades afectadas, mecanismos operativos de reclamación cuya disponibilidad y accesibilidad fueran claras y eficaces;

h) Colaborar con los Gobiernos y la sociedad civil para desarrollar una tecnología que promoviera y afianzara los derechos humanos.

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, Informe de 18 de junio de 2018

99. Los Estados deben, de conformidad con el principio de la debida diligencia, asegurarse de que la reglamentación sobre los intermediarios de Internet respete el marco internacional de derechos humanos, en particular en lo que respecta a las empresas y los derechos humanos, que debería ampliarse para incluir explícitamente los instrumentos relativos a los derechos humanos de la mujer que prohíben la violencia de género en línea.

115. Los intermediarios de Internet deben respetar el principio de que los derechos humanos están protegidos en línea, y aceptar y aplicar voluntariamente todos los instrumentos internacionales fundamentales de derechos humanos y relativos a los derechos de la mujer, con miras a contribuir a la protección universal de los derechos humanos y lograr el empoderamiento de las mujeres, y eliminar la discriminación y la violencia contra ellas en el espacio digital. A este respecto, deben cooperar activamente con los órganos creados en virtud de tratados y los procedimientos especiales, en particular con la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, y con los mecanismos internacionales y regionales independientes relativos a los derechos de la mujer.

116. Los intermediarios deben adoptar mecanismos de denuncia transparentes para los casos de violencia en línea y facilitada por las TIC contra las mujeres y las niñas. Las políticas y los procedimientos para la presentación de denuncias y la solicitud de supresión de contenidos perjudiciales deben ser fácilmente accesibles y transparentes. Los intermediarios deben publicar una política clara y amplia sobre la moderación de los contenidos y salvaguardias de derechos humanos contra la censura arbitraria, y procedimientos de revisión y apelación transparente.

EL DEBER DE LA DEBIDA DILIGENCIA Y LOS INTERMEDIARIOS

Convenio sobre ciberdelincuencia de Budapest, de 23 de noviembre de 2001

2. [C]ada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

50.i) Alentar al sector de las TIC y a los intermediarios de Internet, incluidas las plataformas de redes sociales, a que hagan un esfuerzo activo para evitar los sesgos de género en el diseño de productos inteligentes, aplicaciones para teléfonos móviles y videojuegos, así como en el desarrollo de la inteligencia artificial y, respectivamente, a crear mecanismos de seguimiento interno para garantizar la inclusión de perspectivas centradas en las víctimas, así como para promover una mayor conciencia de la perspectiva y las experiencias de las usuarias, en particular aquellas expuestas o en riesgo de sufrir formas interseccionales de discriminación. Se debería incentivar a los intermediarios de Internet y a las empresas de tecnología para que cooperen con las ONG que trabajan en el tema de la violencia contra las mujeres en sus esfuerzos de sensibilización y otros esfuerzos;

57. [...] h) involucrar al sector de las TIC y a los intermediarios de Internet en los esfuerzos para responsabilizar a los perpetradores de violencia contra las mujeres en la esfera digital sobre la base de sus normas internas y respetando la legislación penal y de otro tipo, en particular mediante:

i. ofrecer mecanismos de denuncia eficaces y fácilmente accesibles para que los usuarios denuncien contenidos nocivos, que sean capaces de responder a dichas solicitudes de manera oportuna y teniendo en cuenta factores que exponen a las mujeres y las niñas de manera desproporcionada al abuso en línea, en particular el sexo, el género, la raza, el color, idioma, religión, opinión política o de otro tipo, origen nacional o social, asociación con una minoría nacional, propiedad, nacimiento, orientación sexual, identidad de género, edad, estado de salud, discapacidad, estado civil, condición de migrante o refugiado, u otra condición;

ii. incentivar actividades comerciales en línea que incorporen una perspectiva de derechos humanos en todas las etapas de su actividad, incluido el diseño de productos, con miras a reducir los riesgos para las mujeres y las niñas, como las que rastrean y espían;

iii. alentar a los proveedores de servicios a que hagan disponible en sus plataformas información legal e información sobre cómo solicitar la eliminación de contenido no consensuado, incluidas imágenes o videos, en idiomas relevantes y apropiados para la base de usuarios;

(i) impedir que entidades comerciales obtengan ganancias del abuso sexual de mujeres y niñas que constituya violencia sexual, como la violación filmada, incluso criminalizando la producción y distribución de dicho contenido [...]

EL DEBER DE LA DEBIDA DILIGENCIA Y LA TRANSPARENCIA

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

55. Los desarrolladores, comercializadores, operadores y usuarios de sistemas de IA deberían aumentar drásticamente sus medidas para promover la transparencia en lo que respecta al uso de estos sistemas. Como primer paso, los Estados, las empresas y otros usuarios de IA deberían facilitar información sobre el tipo de sistemas que utilizan, los fines que persiguen con su uso y la identidad del desarrollador y el operador de los sistemas. Las personas afectadas deben ser informadas sistemáticamente cuando se tomen o se hayan tomado decisiones de forma automática o con la ayuda de herramientas de automatización. También se les debe informar cuando los datos personales que proporcionan pasen a formar parte de un conjunto de datos utilizados por un sistema de IA. [...] Debe garantizarse el cumplimiento efectivo de las obligaciones de transparencia y los derechos de acceso, supresión y rectificación de datos previstos en los marcos de protección de la privacidad de los datos. Debe prestarse especial atención a facilitar que los individuos comprendan y controlen mejor los perfiles recopilados en relación con ellos.

56. [...] El desarrollo y la implantación sistemática de metodologías destinadas a hacer que los sistemas de IA sean más explicables —lo que a menudo se denomina transparencia algorítmica— es de suma importancia para garantizar una protección adecuada de los derechos. Esto resulta crucial cuando la IA se utiliza para determinar cuestiones decisivas en el marco de procesos judiciales o en relación con servicios sociales que son esenciales para el ejercicio efectivo de los derechos económicos, sociales y culturales. [...]

EL DEBER DE DEBIDA DILIGENCIA Y LA COOPERACIÓN INTERNACIONAL ENTRE ESTADOS

Convenio sobre ciberdelincuencia de Budapest, de 23 de noviembre de 2001

Artículo 23. Principios generales relativos a la cooperación internacional.

Las Partes cooperarán entre sí en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Artículo 25. Principios generales relativos a la asistencia mutua.

1. Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.

[...]

3. En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.

4. Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11 únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.

5. Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente.

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

0. Considerando que algunos Estados miembros han adoptado leyes solo sobre algunas formas específicas de ciberviolencia de género y que, por lo tanto, sigue habiendo importantes lagunas; que en la actualidad no existe una definición común ni un enfoque político eficaz para luchar contra la ciberviolencia de género a escala de la Unión; que la falta de esta definición armonizada a escala de la Unión da lugar a diferencias considerables en la medida en que los Estados miembros combaten y previenen la ciberviolencia de género, lo que provoca grandes disparidades y fragmentación en el grado de protección que proporcionan, a pesar del carácter transfronterizo de este delito; que se necesita, por tanto, una definición jurídica armonizada de ciberviolencia de género tanto a escala de la Unión como a escala nacional;

49. Pide una cooperación eficaz entre las autoridades policiales y las empresas tecnológicas y los proveedores de servicios, que deben respetar plenamente los derechos y libertades fundamentales y las normas de protección de datos, con el fin de garantizar la protección de las víctimas y salvaguardar sus derechos;

(En el mismo sentido: Convenio del Consejo de Europa sobre prevención y lucha contra las mujeres y la violencia doméstica (Convenio de Estambul), de 2011, artículo 62).

B) El deber de prevención

EL DEBER DE PREVENCIÓN RESPECTO DE LA VIOLENCIA EN LÍNEA

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, Informe de 18 de junio de 2018

66. La prevención incluye medidas para crear conciencia sobre la violencia contra las mujeres y las niñas facilitada por las TIC como formas de violencia contra la mujer, así como para establecer y proporcionar información sobre los servicios y la protección jurídica de que disponen para poner fin a las violaciones y evitar que se repitan. Los Estados están obligados a adoptar las medidas necesarias para prevenir las violaciones de los derechos humanos cometidas en el extranjero por intermediarios de Internet sobre los que puedan ejercer influencia, ya sea a través de medios reglamentarios o del uso de incentivos.

Recomendación general nº 35 del Comité CEDAW, sobre la violencia por razón de género contra la mujer, por la que se actualiza la Recomendación General nº 19, de 26 de julio de 2017

30. El Comité recomienda que los Estados partes apliquen las siguientes medidas preventivas: [...]

Aprobar y aplicar medidas eficaces para alentar a los medios de comunicación a que eliminen la discriminación contra la mujer, en particular la divulgación de una imagen perjudicial y estereotipada de las mujeres o de determinados grupos de mujeres, como las defensoras de los derechos humanos, de sus actividades, prácticas y resultados, por ejemplo en la publicidad, en línea y en otros entornos digitales. Las medidas deberían incluir lo siguiente:

I) Alentar la creación o el fortalecimiento de mecanismos de autorregulación por parte de organizaciones de medios de comunicación, incluidas organizaciones de medios de comunicación en línea o de medios sociales, encaminados a la eliminación de los estereotipos de género relativos a las mujeres y los hombres o a grupos específicos de mujeres, y abordar la violencia por razón de género contra la mujer que se produce a través de sus servicios y plataformas;

II) Directrices para la cobertura adecuada por parte de los medios de comunicación de los casos de violencia por razón de género contra la mujer;

III) El establecimiento o el fortalecimiento de la capacidad de las instituciones nacionales de derechos humanos para supervisar o examinar las denuncias relacionadas con cualquier medio de comunicación que difunda imágenes o contenido discriminatorios por razón de género que traten a las mujeres como objetos o las degraden o promuevan la masculinidad violenta;

EL DEBER DE PREVENCIÓN RESPECTO DE LA VIOLENCIA EN LÍNEA

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

51. GREVIO recomienda que los Estados Partes implementen las siguientes medidas preventivas:

a) Consideren revisar cualquier legislación relevante vigente y adopten nueva legislación cuando sea necesario para prevenir, brindar protección y procesar la dimensión digital de la violencia contra las mujeres en contra de los estándares de Estambul. Convenio y otras normas pertinentes, incluido el Convenio de Budapest;

b) Emprender iniciativas destinadas a erradicar los estereotipos de género, las actitudes sexistas y la discriminación contra las mujeres que se manifiestan tanto en línea como fuera de línea, teniendo en cuenta la Recomendación CM/Rec(2019)1 del Comité de Ministros del Consejo de Europa sobre prevención y lucha contra el sexismo;

c) Fomentar la igualdad de género en la sociedad y apoyar el empoderamiento y la representación de las mujeres en línea mejorando la alfabetización digital y la participación de todas las mujeres y niñas;

d) Alentar a todos los miembros de la sociedad, especialmente hombres y niños, a abandonar los estereotipos nocivos de mujeres y hombres y adoptar comportamientos respetuosos y saludables en la esfera digital; [...]

LA TIPIFICACIÓN DE LAS CONDUCTAS PUNIBLES COMO PARTE DEL DEBER DE PREVENCIÓN RESPECTO DE LA VIOLENCIA EN LÍNEA

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, Informe de 18 de junio de 2018

79. [M]uchos Estados no disponen de un marco jurídico integral para combatir y prevenir la violencia contra la mujer, en particular con respecto a disposiciones específicas sobre la violencia en línea contra la mujer y facilitada por las TIC, y tampoco se han adherido a todos los tratados fundamentales de derechos humanos. [...]

81. [...] Cuando no existe un derecho especializado, las víctimas se ven obligadas a demandar a los autores a través de diversos delitos conexos que tal vez no sean suficientes; [...]

82. [...] Sin penalización, las víctimas no pueden proteger sus derechos humanos a la intimidad y la dignidad. Incluso en los casos en que las leyes penales tipifican específicamente como delito la distribución no consentida de imágenes sexualmente explícitas, muchas de estas leyes tienen deficiencias; por ejemplo, muchas leyes penales exigen pruebas de la intención de causar daño o malestar psíquico a la víctima, lo que podría ser complicado de demostrar y dificulta el logro de condenas. [...]

LA TIPIFICACIÓN DE LAS CONDUCTAS PUNIBLES COMO PARTE DEL DEBER DE PREVENCIÓN RESPECTO DE LA VIOLENCIA EN LÍNEA

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

En particular, los Estados deben tipificar como delito la distribución no consensuada de imágenes íntimas, incluyendo sus distintas modalidades y manifestaciones, los grados de participación de los responsables, el tipo de contenidos perjudiciales, su posterior difusión y la ilegalidad de las amenazas de divulgación no consentida de dichos materiales. Además, se debe colocar especial atención en que las normas no incorporen descripciones confusas o conceptos que impliquen una estigmatización de la expresión sexual de las víctimas.

Los Estados deberán también prohibir claramente y penalizar otros actos graves de violencia de género como el ciberacoso y el ciberhostigamiento, señalando como una agravante el que estos actos se realicen en el marco de una relación sexo-afectiva o en contextos de violencia doméstica o de pareja.

Los Estados deben también brindar otras alternativas a la vía penal para que las mujeres víctimas accedan a la justicia, como por ejemplo procedimientos civiles a través de demandas por daños y perjuicios, administrativos o laborales para casos de ciberhostigamiento y ciberacoso sexual en el marco de relaciones de trabajo. (Pág. 90)

Relator Especial sobre el derecho a la privacidad, Informe de 24 de marzo de 2020

44. Los Estados deberían:

a) Reconocer la violencia en línea en razón del género como una violación de los derechos humanos y una forma de discriminación y adoptar medidas para aplicar los instrumentos internacionales de derechos humanos, en conjunción con las leyes nacionales, a fin de prevenir y mitigar su aparición;

[...]

c) Reformar las leyes penales y civiles para hacer frente a la violencia facilitada por la tecnología y establecer causas penales y civiles que permitieran a las víctimas buscar reparación con una protección adecuada de su privacidad para prevenir la victimización secundaria y dotarlas de mayor control;

[...]

o) Prohibir y tipificar como delito la distribución no consentida de imágenes íntimas en espacios digitales y fuera de línea, por medio de legislación que abarcara todos los elementos de este tipo de abuso:

I) Sin limitar el alcance a las parejas íntimas actuales o anteriores o a los géneros binarios;

II) Penalizando la distribución o redistribución de esas imágenes;

III) Protegiendo a las víctimas de imágenes que representaran actos o conductas sexuales, no solo la desnudez, y de las llamadas falsificaciones pornográficas;

IV) Haciendo ilegal la amenaza de difundir imágenes íntimas no consentidas;

LA TIPIFICACIÓN DE LAS CONDUCTAS PUNIBLES COMO PARTE DEL DEBER DE PREVENCIÓN RESPECTO DE LA VIOLENCIA EN LÍNEA

V) Permitiendo a las víctimas solicitar al tribunal una orden de supresión del contenido perjudicial, además de una orden provisional para que el autor dejara de distribuir el material rápidamente, hasta tanto se resolviera la causa judicial, en colaboración con los intermediarios de Internet;

VI) Realizando investigaciones de manera oportuna y firme y aplicando sanciones a las personas condenadas por esos abusos; [...]

(En el mismo sentido: Comisión Africana de Derechos Humanos y de los Pueblos, Resolución sobre la protección de las mujeres contra la violencia digital en África - ACHPR/Res. 522 (LXXII), de 11 de agosto de 2022).

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

23. [...] La Relatora Especial formuló una serie de recomendaciones para los Estados, incluidas las recomendaciones de que los Estados deberían prohibir claramente y criminalizar la violencia en línea contra las mujeres, en particular la distribución no consensuada de imágenes íntimas y la amenaza de difundir tales imágenes [...].

(En el mismo sentido: TEDH, Caso Buturuga vs. Rumanía, Sentencia de 11 de febrero de 2020, párr. 20).

TEDH, Caso K.U. vs. Finlandia, Sentencia de 2 de marzo de 2009

46. El Gobierno admitió que, en ese momento, no se podía ordenar al operador del servidor de Internet que proporcionara información que identificara al delincuente. Sostuvieron que la protección se obtenía por la mera existencia del delito de tergiversación maliciosa y por la posibilidad de presentar cargos penales o una acción por daños y perjuicios contra el operador del servidor. En cuanto a lo primero, el Tribunal observa que la existencia de un delito tiene efectos disuasorios limitados si no hay medios para identificar al verdadero infractor y llevarlo ante la justicia. En este caso, el Tribunal observa que no ha excluido la posibilidad de que las obligaciones positivas del Estado en virtud del artículo 8 de salvaguardar la integridad física o moral del individuo puedan extenderse a cuestiones relativas a la eficacia de una investigación penal, incluso cuando la responsabilidad penal de los agentes del Estado no está en cuestión. Para la Corte, los Estados tienen la obligación positiva inherente al artículo 8 de la Convención de penalizar los delitos contra la persona, incluidas las tentativas de delito, y de reforzar el efecto disuasorio de la penalización aplicando en la práctica las disposiciones del derecho penal mediante una investigación y un enjuiciamiento efectivos.

47. En cuanto al argumento del Gobierno de que el demandante tenía la posibilidad de obtener daños y perjuicios de un tercero, a saber, el proveedor de servicios, el Tribunal considera que no era suficiente en las circunstancias de este caso. Es claro que tanto el interés público como la protección de los intereses de las víctimas de crímenes cometidos contra su bienestar físico o psicológico requieren la disponibilidad de un recurso que permita identificar al verdadero culpable y llevarlo ante la justicia, en el presente caso el persona que colocó el anuncio a nombre del demandante, y a la víctima a obtener de él una reparación económica.

LA REGULACIÓN DE APLICACIONES, SISTEMAS Y USOS DE LA INTELIGENCIA ARTIFICIAL DEBE SER ESPECÍFICA Y PROPORCIONADA

ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021

45. Teniendo en cuenta la diversidad de aplicaciones, sistemas y usos de la IA, la regulación debe ser lo suficientemente específica como para abordar los problemas propios de cada sector y adaptar las respuestas a los riesgos que puedan plantearse. Cuanto mayor sea el riesgo para los derechos humanos, más estrictos deben ser los requisitos legales para el uso de la tecnología de IA. Por lo tanto, los sectores en los que están más en juego los intereses de las personas, como la aplicación de la ley, la seguridad nacional, la justicia penal, la protección social, el empleo, la atención de la salud la educación y el sector financiero, deberían ser prioritarios. Un enfoque de la legislación y la reglamentación proporcionado a los riesgos exigirá la prohibición de determinadas tecnologías, aplicaciones o usos de la IA si tienen efectos potenciales o reales que no están justificados en virtud del derecho internacional de los derechos humanos, en particular si no superan las pruebas de necesidad y proporcionalidad. Además, los usos de la IA que son intrínsecamente incompatibles con la prohibición de la discriminación, no deberían autorizarse. [...]

EL DEBER DE PREVENCIÓN Y EL DERECHO A LA INFORMACIÓN Y A LA EDUCACIÓN

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

18. Anima a los Estados miembros a que adopten y apliquen debidamente y de forma eficaz el Derecho nacional adecuado, también en materia de justicia penal, y políticas específicas para promover la concienciación y para crear campañas, programas educativos y de formación, también sobre educación, alfabetización y competencias digitales, que se dirijan igualmente a las generaciones más jóvenes; anima a la Comisión a que apoye a los Estados miembros a este respecto;

19. Destaca la importancia de la igualdad de género en los planes de estudios para abordar las causas profundas de la violencia de género eliminando los estereotipos de género y cambiando las actitudes sociales y culturales que conducen a normas sociales y de género dañinas; subraya el papel de los formadores cualificados, como el personal docente, a la hora de apoyar a los estudiantes en las cuestiones relacionadas con la ciberviolencia de género, así como la importancia de invertir en dichos formadores; señala que debe prestarse especial atención a la educación de niños y hombres;

26. Pide a la Comisión que promueva campañas de concienciación, información y defensa que aborden la ciberviolencia de género en todas sus formas y ayuden a garantizar un espacio público digital seguro para todos; considera que una campaña de concienciación a escala de la Unión sobre la ciberviolencia de género debe incluir, entre otras cosas, información destinada a enseñar a los ciudadanos más jóvenes de la Unión cómo reconocer las distintas formas de ciberviolencia y cómo denunciarlas, así como información en materia de derechos digitales; señala que la ciberviolencia de género afecta especialmente a las mujeres jóvenes y pide, a este respecto, que se desarrollen iniciativas específicas de prevención y concienciación;

(En el mismo sentido: GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, párrs. 50.e, f y g).

Ley 27736, de modificaciones de la Ley 26485 (Ley Olimpia-Argentina), de 23 de octubre de 2023

Artículo 5.o)

Implementar un servicio multisoporte, telefónico y digital gratuito y accesible, en forma articulada con las provincias, a través de organismos gubernamentales pertinentes, destinada a dar contención, información y brindar asesoramiento sobre recursos existentes en materia de prevención de la violencia contra las mujeres y asistencia a quienes la padecen, incluida la modalidad de 'violencia contra las mujeres en el espacio público' conocida como 'acoso callejero'. [...]

Artículo 6.f)

Promover programas de alfabetización digital, buenas prácticas en el uso de las tecnologías de la información y la comunicación y de identificación de las violencias digitales, en las clases de educación sexual integral como en el resto de los contenidos en el ámbito educativo y en la formación docente.

EL DEBER DE PREVENCIÓN Y LA EXIGENCIA DE UN MARCO SÓLIDO Y COORDINADO DE RECOPILACIÓN DE DATOS

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

AA. Considerando que, para erradicar la violencia de género, incluida la ciberviolencia de género, es necesario apoyarse en datos administrativos coherentes, concretos, representativos y comparables, basados en un marco sólido y coordinado de recopilación de datos; que faltan datos desglosados exhaustivos y comparables sobre todas las formas de violencia de género y sus causas profundas; que, a pesar de la creciente concienciación respecto a este fenómeno, la falta de recopilación de datos sobre todas las formas de violencia de género impide una evaluación precisa de su incidencia; que la indisponibilidad de datos está vinculada a la infranotificación de los casos de ciberviolencia de género; que el Convenio de Estambul y la Directiva 2012/29/UE exigen a los Estados miembros que notifiquen datos estadísticos y elaboren datos desglosados por género;

27. Insta a la Comisión y a los Estados miembros a que establezcan un sistema fiable para recopilar periódicamente datos estadísticos desglosados, comparables y pertinentes sobre la violencia de género a escala de la Unión, incluidas la ciberviolencia y su prevalencia, dinámica y consecuencias, y a que desarrollen indicadores que permitan medir los progresos realizados; reafirma la necesidad de recopilar datos exhaustivos, desglosados y comparables, incluidos datos científicos, a fin de calibrar la magnitud de la violencia de género, encontrar soluciones y medir los progresos realizados; [...]

Ley 27736, de modificaciones de la Ley 26485 (Ley Olimpia-Argentina), de 23 de octubre de 2023

Artículo 5.o)

[...] La información recabada por las denuncias efectuadas a este servicio debe ser recopilada y sistematizada por la autoridad de aplicación a fin de elaborar estadísticas confiables para la prevención y erradicación de las diversas modalidades de violencia contra las mujeres.

C) El deber de protección

EL DEBER DE PROTECCIÓN ES UNA OBLIGACIÓN DE MEDIOS Y NO DE RESULTADOS

TEDH, Caso K.U. vs. Finlandia, Sentencia de 2 de marzo de 2009

48. El Tribunal acepta que, en vista de las dificultades que implica la vigilancia de las sociedades modernas, una obligación positiva debe interpretarse de manera que no imponga una carga imposible o desproporcionada a las autoridades o, como en este caso, al legislador. [...]

EL DEBER DE PROTECCIÓN CONLLEVA IMPLEMENTAR MEDIDAS ADECUADAS, PRÁCTICAS, EFECTIVAS Y EN DIFERENTES ÁMBITOS

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

(Considerando 53) Las medidas con el fin de eliminar de inmediato el material o de inhabilitar el acceso al material deben incluir, en particular, facultar a las autoridades nacionales para dictar órdenes a los prestadores de servicios de alojamiento de datos para que eliminen uno o más elementos específicos del material en cuestión, o inhabiliten el acceso a ellos. Las autoridades nacionales también deben poder dictar órdenes de inhabilitación del acceso destinadas a otros prestadores de servicios intermediarios pertinentes.

(En el mismo sentido: OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022, pág. 118).

EL DEBER DE PROTECCIÓN RESPECTO DE LA VIOLENCIA EN LÍNEA

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, Informe de 18 de junio de 2018

67. La obligación de proteger a las víctimas de la violencia en línea contra la mujer abarca el establecimiento de procedimientos para la supresión inmediata de un contenido perjudicial por motivos de género mediante la eliminación del material original o de su distribución. La protección también requiere la adopción de medidas judiciales inmediatas por conducto de órdenes judiciales nacionales y la rápida intervención de los intermediarios de Internet y, en algunos casos, también puede requerir la cooperación extraterritorial. Incluye la prestación de servicios accesibles para supervivientes, como servicios de asistencia jurídica. La protección entraña además la obligación de los Estados de adoptar medidas positivas para erradicar todas las formas de violencia, incluidas las manifestaciones de violencia en línea, aunque una persona no haya presentado una denuncia (por ejemplo, en el caso de los foros en línea que en general promueven la violencia contra la mujer).

CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018

[E]l carácter multijurisdiccional y transnacional de la violencia contra las mujeres y las niñas en los contextos digitales, y la utilización y adaptación continuas de las tecnologías digitales por los autores de esos actos para evitar la detección y la investigación, exigen una cooperación activa entre los distintos actores, incluidos los Estados, sus fuerzas del orden y autoridades judiciales, y los actores del sector privado en lo que respecta a la detección de delitos, su denuncia ante las autoridades competentes para su investigación, la preservación de las pruebas electrónicas de los delitos y la entrega de las pruebas a las autoridades de manera oportuna. (Págs. 3-4)

TEDH, Caso Volodina vs. Rusia (nº 2), Sentencia de 14 de septiembre de 2021

23. [...] La Relatora Especial formuló una serie de recomendaciones para los Estados, incluidas las recomendaciones de que los Estados deberían prohibir claramente y criminalizar la violencia en línea contra las mujeres, en particular [...] que los Estados deberían permitir que las víctimas obtengan órdenes de protección para evitar que sus abusadores publiquen o compartan imágenes íntimas sin su consentimiento [...].

49. [...] Los Estados tienen la obligación positiva de establecer y aplicar de manera efectiva un sistema que castigue todas las formas de violencia doméstica y de brindar garantías suficientes para las víctimas. [...]

(En el mismo sentido: TEDH, Caso Buturuga vs. Rumanía, Sentencia de 11 de febrero de 2020, párrs. 74-78).

EL DEBER DE PROTECCIÓN RESPECTO DE LA VIOLENCIA EN LÍNEA

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

53. GREVIO recomienda que los Estados Partes implementen las siguientes medidas de protección:

a) garantizar que el marco legal relacionado con la violencia contra las mujeres se refiera y se aplique a todas las formas de violencia cometida en la esfera digital, respete el principio de diligencia debida establecido en el artículo 5 Convenio de Estambul y facilita el diálogo formal e informal entre los organismos responsables de responder a las víctimas. La respuesta debe ser sensible al género e integrar las especificidades de la dimensión digital de la violencia contra las mujeres;

b) desarrollar y difundir información accesible sobre las vías legales y los servicios de apoyo disponibles para las víctimas de la violencia contra las mujeres perpetrada en la esfera digital y crear mecanismos de denuncia en línea y fuera de línea dentro de los servicios policiales y de fiscalía que sean fácil e inmediatamente accesibles para las víctimas, incluyendo aquellos con discapacidad física, así como intelectual y psicosocial, que cumplan con las normas internacionales y nacionales de protección de datos, en línea con el Convenio Modernizado del Consejo de Europa para la Protección de las Personas con respecto al Procesamiento Automático de Datos Personales (CETS No. 223);

c) hacer que los servicios de apoyo, incluido el asesoramiento jurídico y psicológico, sean accesibles a todas las víctimas de la violencia contra las mujeres perpetrada en la esfera digital, incluida la violencia perpetrada en el contexto de la violencia doméstica, dotando a los servicios de apoyo especializados para mujeres existentes y a otros servicios con experiencia en dotar a este sector de los recursos financieros y humanos para ofrecer servicios integrales, incluido asesoramiento jurídico y técnico sobre la eliminación de contenidos nocivos en línea;

d) permitir, a través de la capacitación, el desarrollo de capacidades y recursos suficientes, servicios de apoyo generales y especializados para las mujeres víctimas de violencia, incluidos refugios y servicios de asesoramiento no residenciales, apoyo económico temporal destinado a su autosuficiencia y autonomía a corto plazo, así como como servicios sociales y de atención de salud, para tomar conciencia y responder a las experiencias de violencia digital de mujeres y niñas;

e) dotar a las líneas telefónicas nacionales de ayuda establecidas de conformidad con el artículo 24 del Convenio de Estambul de los recursos y la experiencia necesarios para responder a la dimensión digital de la violencia contra las mujeres y garantizar su accesibilidad para todas las víctimas, independientemente de los factores que puedan exponerlas a múltiples formas de discriminación;

f) empoderar a los órganos de igualdad y a las instituciones de defensa del pueblo de los Estados Partes que tienen el mandato de trabajar en materia de igualdad de género y no discriminación para abordar la dimensión digital de la violencia contra las mujeres desde el punto de vista de la discriminación estructural y la barrera para la realización de los derechos de las mujeres. derechos humanos que pueda representar; y

g) incentivar a los intermediarios de Internet, incluidos los ISP, los motores de búsqueda y las plataformas de redes sociales, para garantizar una moderación sólida del contenido que entra dentro del alcance del Convenio de Estambul mediante la eliminación de cuentas o contenidos, en múltiples idiomas, sobre la base de principios transparentes que protejan la derechos humanos de todos, incluido el derecho de las mujeres a vivir libres de violencia y proporcionar orientación de fácil acceso a los usuarios para denunciar contenidos abusivos y solicitar su eliminación.

MEDIDAS ESPECÍFICAS DE PROTECCIÓN

Ley de acceso de las mujeres a una vida libre de violencia (Ley Olimpia-México), de 1 de junio de 2021

Artículo 20 sexies.

Tratándose de violencia digital o mediática para garantizar la integridad de la víctima, la o el Ministerio Público, la jueza o el juez, ordenarán de manera inmediata, las medidas de protección necesarias, ordenando vía electrónica o mediante escrito a las empresas de plataformas digitales, de medios de comunicación, redes sociales o páginas electrónicas, personas físicas o morales, la interrupción, bloqueo, destrucción, o eliminación de imágenes, audios o videos relacionados con la investigación previa satisfacción de los requisitos de Ley.

En este caso se deberá identificar plenamente al proveedor de servicios en línea a cargo de la administración del sistema informático, sitio o plataforma de Internet en donde se encuentre alojado el contenido y la localización precisa del contenido en Internet, señalando el Localizador Uniforme de Recursos.

La autoridad que ordene las medidas de protección contempladas en este artículo deberá solicitar el resguardo y conservación lícita e idónea del contenido que se denunció de acuerdo a las características del mismo.

Las plataformas digitales, medios de comunicación, redes sociales o páginas electrónicas darán aviso de forma inmediata al usuario que compartió el contenido, donde se establezca de forma clara y precisa que el contenido será inhabilitado por cumplimiento de una orden judicial.

Dentro de los cinco días siguientes a la imposición de las medidas de protección previstas en este artículo deberá celebrarse la audiencia en la que la o el juez de control podrá cancelarlas, ratificarlas o modificarlas considerando la información disponible, así como la irreparabilidad del daño.

Ley 27736, de modificaciones de la Ley 26485 (Ley Olimpia-Argentina), de 23 de octubre de 2023

Artículo 10. [...]

a.2. Ordenar al presunto agresor que cese en los actos de perturbación o intimidación que, directa o indirectamente, realice hacia la mujer, tanto en el espacio analógico como en el digital.

Artículo 11. [...]

a.8. Ordenar la prohibición de contacto del presunto agresor hacia la mujer que padece violencia por intermedio de cualquier tecnología de la información y la comunicación, aplicación de mensajería instantánea o canal de comunicación digital.

Artículo 12. [...]

a.9. Ordenar por auto fundado, a las empresas de plataformas digitales, redes sociales, o páginas electrónicas, de manera escrita o electrónica la supresión de contenidos que constituyan un ejercicio de la violencia digital o telemática definida en la presente ley, debiendo identificarse en la orden la URL específica del contenido cuya remoción se ordena. A los fines de notificación de la medida del presente inciso se podrá aplicar el artículo 122 de la ley 19.550

MEDIDAS ESPECÍFICAS DE PROTECCIÓN

La autoridad interviniente en el caso deberá solicitar a las empresas de plataformas digitales, redes sociales, o páginas electrónicas, el aseguramiento de los datos informáticos relativos al tráfico, a los abonados y contenido del material suprimido, que obren en su poder o estén bajo su control, para las acciones de fondo que correspondan, durante un plazo de noventa (90) días que podrá renovarse una única vez por idéntico plazo a pedido de la parte interesada. Se deberá ordenar mantener en secreto la ejecución de dicho procedimiento mientras dure la orden de aseguramiento.

La autoridad podrá, a requerimiento de parte y únicamente para la investigación de las acciones de fondo que correspondan, solicitar a las requeridas que revelen los datos informáticos de abonados que obren en su poder o estén bajo su control e igualmente los relativos al tráfico y al contenido del material suprimido mediante auto fundado de acuerdo a los mecanismos de cooperación interna y/o procedimientos previstos en el marco de las normas y tratados sobre cooperación internacional vigentes.

MEDIDAS PARA LA ELIMINACIÓN DEL MATERIAL ILÍCITAMENTE CREADO/OBTENIDO Y DIVULGADO EN LÍNEA

Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, de 2024

Artículo 23. Medidas para eliminar determinado material en línea.

1. Sin perjuicio de lo dispuesto en el Reglamento (UE) 2022/2065, los Estados miembros adoptarán las medidas necesarias para garantizar que el material en línea accesible públicamente a que se refieren el artículo 5, apartado 1, letras a) y b), y los artículos 7 y 8 de la presente Directiva se elimine rápidamente o que se inhabilite el acceso a él.

Las medidas a que se refiere el párrafo primero del presente apartado incluirán la posibilidad de que las autoridades competentes dicten órdenes jurídicamente vinculantes para que se elimine dicho material o se inhabilite el acceso a él. Los Estados miembros velarán por que dichas órdenes cumplan, como mínimo, las condiciones establecidas en el artículo 9, apartado 2, del Reglamento (UE) 2022/2065.

2. Las órdenes a que se refiere el apartado 1, párrafo segundo, se dirigirán a los prestadores de servicios de alojamiento de datos.

Cuando la eliminación no sea factible, las autoridades competentes también podrán dirigir órdenes de inhabilitación del acceso al material en cuestión a prestadores de servicios intermediarios pertinentes distintos de los prestadores de servicios de alojamiento de datos, que tengan la capacidad técnica y operativa para tomar medidas con respecto al material en cuestión.

3. Los Estados miembros velarán por que, cuando los procesos penales relativos a un delito contemplado en el artículo 5, apartado 1, letras a) o b), o en los artículos 7 u 8 concluyan sin que se declare que se haya cometido un delito, las órdenes a que se refiere el apartado 1, párrafo segundo, del presente artículo sean revocadas y se informe de ello a los destinatarios de dichas órdenes.

4. Los Estados miembros se asegurarán de que las órdenes y otras medidas a las que se refiere el apartado 1 se adopten con arreglo a procedimientos transparentes y sean objeto de las salvaguardias adecuadas, en particular para garantizar que dichas órdenes y otras medidas se limiten a lo que sea necesario y proporcionado y que se tengan debidamente en cuenta los derechos e intereses de todas las partes implicadas pertinentes, incluidos sus derechos fundamentales en virtud de la Carta.

Los Estados miembros se asegurarán de que los prestadores de servicios de alojamiento de datos, otros prestadores de servicios intermediarios pertinentes y los proveedores de contenidos afectados por alguna de las órdenes a que se refiere el apartado 1, párrafo segundo, tengan derecho a tutela judicial efectiva. Dicho derecho incluirá el derecho a impugnar dicha orden ante los órganos jurisdiccionales del Estado miembro de la autoridad competente que la haya dictado.

5. Los Estados miembros se asegurarán de que los proveedores de contenido pertinentes afectados por alguna de las órdenes a que se refiere el apartado 1, párrafo primero, sean informados, cuando proceda, por los prestadores de servicios de alojamiento de datos o por cualquier otro prestador de servicios intermediarios pertinente afectado, de las razones de la eliminación del material o la inhabilitación del acceso a él en virtud de las órdenes u otras medidas a que se refiere el apartado 1 y de la posibilidad de tener acceso a tutela judicial.

6. Los Estados miembros se asegurarán de que la eliminación del material o la inhabilitación del acceso a él en virtud de las órdenes u otras medidas a que se refiere el apartado 1 no impidan a las autoridades competentes obtener o asegurar, sin demora indebida, las pruebas necesarias para la investigación y el enjuiciamiento de los delitos a que se refieren el artículo 5, apartado 1, letras a) y b), y los artículos 7 y 8.

D) El deber de investigación y enjuiciamiento

EL DEBER DE INVESTIGACIÓN Y ENJUICIAMIENTO DE LOS CASOS DE VIOLENCIA EN LÍNEA

TEDH, Caso Volodina vs. Rusia, Sentencia de 4 de noviembre de 2019

92 [...] La obligación del Estado de investigar no se cumplirá si la protección que otorga el derecho interno existe solo en la teoría; sobre todo, también debe operar de manera efectiva en la práctica, y eso requiere un rápido examen del caso sin demoras innecesarias.

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, Informe de 18 de junio de 2018

68. El enjuiciamiento consiste en la investigación y la interposición de actuaciones penales contra los autores. Con frecuencia, los órganos encargados de hacer cumplir la ley trivializan la violencia en línea contra la mujer, y sus acciones lamentablemente a menudo se caracterizan por la culpabilización de las víctimas en relación con estos casos. Esta actitud se traduce en una cultura de silencio y en la denuncia insuficiente de casos pues las mujeres víctimas se resisten a hablar por temor a ser culpadas. Aun en los casos en que las mujeres presentan denuncias y se inician investigaciones, tropiezan con nuevos obstáculos debido a la falta de conocimientos técnicos y de capacidad en el poder judicial (incluidos los sistemas judiciales, los magistrados y los jueces). Además, las costas de los litigios impiden que muchos supervivientes, en particular las mujeres más pobres, presenten sus causas ante los tribunales. Por lo tanto, es fundamental evaluar la labor de los equipos de respuesta inicial —incluidos los intermediarios de Internet, la policía y las líneas telefónicas de asistencia— y del poder judicial y los organismos reguladores a fin de obtener una descripción fiel de la realidad de las experiencias de las mujeres y facilitar su acceso a la justicia y los recursos.

TEDH, K.U. vs. Finlandia, Sentencia de 2 de marzo de 2009.

49. El Tribunal considera que la protección práctica y efectiva del demandante requería que se tomaran medidas efectivas para identificar y procesar al autor, es decir, la persona que colocó el anuncio. En el presente caso, no se brindó dicha protección. [D]icho marco no estaba vigente en el momento de los hechos, por lo que no podía cumplirse la obligación positiva de Finlandia respecto del demandante. Esta deficiencia fue subsanada posteriormente. Sin embargo, los mecanismos introducidos por la Ley de ejercicio de la libertad de expresión en los medios de comunicación llegaron demasiado tarde para el demandante.

OEA-CIM-MESECVI y ONU Mujeres, In forme "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará, de 2022

[E]n casos de violencia de género contra las mujeres facilitada por las TIC, las autoridades deben llevarla [la investigación] a cabo de forma seria, imparcial, efectiva, orientada a la determinación de la verdad y con una perspectiva de género. Asimismo, las víctimas de violencia digital deben contar con amplias posibilidades de ser escuchadas y actuar en los procesos de esclarecimiento de los hechos, de sanción de los responsables y de reparación.

EL DEBER DE INVESTIGACIÓN Y ENJUICIAMIENTO DE LOS CASOS DE VIOLENCIA EN LÍNEA

Además, considerando la prevalencia de la violencia en línea contra mujeres y niñas, en el marco de las obligaciones de debida diligencia reforzada los Estados deben asegurar que autoridades policiales, fiscales y judiciales respondan de forma coordinada, pronta e inmediata, y que existan los mecanismos de denuncia adecuados. (Págs. 118-119)

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

55. GREVIO recomienda que los Estados Partes implementen las siguientes medidas con respecto al enjuiciamiento y castigo de la violencia de género contra las mujeres.

a) dotar a las fuerzas del orden y a otros agentes de la justicia penal de los recursos humanos, financieros y técnicos necesarios para investigar y enjuiciar eficazmente la dimensión digital de la violencia contra las mujeres, de conformidad con sus obligaciones de debida diligencia en virtud del artículo 5 del Convenio de Estambul [...];

b) aumentar los esfuerzos de creación de capacidad para los profesionales de la justicia penal y las fuerzas del orden para dotarlos de la experiencia y los recursos necesarios sobre cómo utilizar los marcos legales existentes para abordar la dimensión digital de la violencia contra las mujeres, así como para desarrollar sus capacidades forenses. sobre la recopilación y protección de pruebas electrónicas sin causar una victimización secundaria y una nueva traumatización de la víctima [...];

c) garantizar la publicación de informes de incidencia por parte del sector de justicia penal sobre la violencia contra las mujeres perpetrada en la esfera digital e información adicional sobre detenciones, acusaciones, condenas y sentencias, así como información sobre sexo, edad, tipo de violencia, así como la relación del autor con la víctima, ubicación geográfica y otros factores que los Estados Partes consideren pertinentes con miras a fortalecer la confianza de las víctimas en el sistema de justicia penal, siempre que la publicación de dicha información no comprometa la presunción de inocencia;

d) garantizar que las víctimas de violencia contra las mujeres perpetrada en la esfera digital tengan acceso efectivo a los sistemas de justicia penal y que las autoridades respondan adecuadamente a esos casos, incluso mediante la aplicación del derecho penal y, según corresponda, el enjuiciamiento de oficio;

e) garantizar que las órdenes de prohibición de emergencia y las órdenes de protección respondan a las formas de violencia doméstica perpetradas en línea o a través de las TIC y a otras manifestaciones digitales de violencia contra las mujeres; y

f) tomar medidas para poner fin a la impunidad de los actos digitales de violencia contra las mujeres fomentando la responsabilidad de todos los actores relevantes, incluidas las empresas de TIC y los intermediarios de Internet, en particular mediante una fuerte moderación y eliminación de contenidos; y alentando a las empresas de medios a trabajar en colaboración con las agencias encargadas de hacer cumplir la ley.

EL DEBER DE SANCIONAR

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, Informe de 18 de junio de 2018

69. El castigo conlleva la obligación de sancionar a los responsables por sus delitos mediante penas que sean necesarias y proporcionales al hecho delictivo. La seguridad del castigo adecuado transmite el mensaje de que no se tolerará la violencia contra las mujeres y las niñas facilitada por las TIC, lo cual es especialmente importante para las mujeres víctimas de la violencia en línea, que con frecuencia no reciben una respuesta eficaz de las autoridades estatales y perciben una cultura de impunidad para los autores.

Convenio sobre ciberdelincuencia de Budapest, de 23 de noviembre de 2001

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Cada Parte garantizará la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

Convenio del Consejo de Europa sobre prevención y lucha contra las mujeres y la violencia doméstica (Convenio de Estambul), de 2011

Artículo 47. Condenas en otra parte.

Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para considerar la posibilidad de tener en cuenta, en el marco de la apreciación de la pena, las condenas firmes dictadas en otra de las Partes por los delitos previstos en el presente Convenio.

ERRADICACIÓN DE LA CULTURA, LA COSTUMBRE, LA RELIGIÓN O EL SUPUESTO HONOR COMO JUSTICACIÓN DE LOS ACTOS DE VIOLENCIA EN EL ÁMBITO DE LAS TIC

Convenio del Consejo de Europa sobre prevención y lucha contra las mujeres y la violencia doméstica (Convenio de Estambul), de 2011

Artículo 46. Justificación inaceptable de los delitos penales, incluidos los delitos cometidos supuestamente en nombre del «honor»

1. Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para garantizar que, en los procedimientos penales abiertos por la comisión de uno de los actos de violencia incluidos en el ámbito de aplicación del presente Convenio, no se considere a la cultura, la costumbre, la religión, la tradición o el supuesto «honor» como justificación de dichos actos. Ello abarca, en especial, las alegaciones según las cuales la víctima habría transgredido las normas o costumbres culturales, religiosas, sociales o tradicionales relativas a un comportamiento apropiado.

2. Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que la incitación hecha por cualquier persona a un menor para que cometa cualquiera de los actos mencionados en el apartado 1 no disminuya la responsabilidad penal de dicha persona en relación con los actos cometidos.

PROHIBICIÓN DE MODOS ALTERNATIVOS DE RESOLUCIÓN DE CONFLICTOS O DE IMPOSICIÓN DE CONDENAS

Convenio del Consejo de Europa sobre prevención y lucha contra las mujeres y la violencia doméstica (Convenio de Estambul), de 2011

Artículo 48.1. Prohibición de modos alternativos obligatorios de resolución de conflictos o imposición de condenas.

1. Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para prohibir los modos alternativos obligatorios de resolución de conflictos, incluidas la mediación y la conciliación, en lo que respecta a todas las formas de violencia incluidas en el ámbito de aplicación del presente Convenio.

E) El deber de reparación

EL DERECHO A LA REPARACIÓN DE LAS VÍCTIMAS DE LA VIOLENCIA EN LÍNEA

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, Informe de 18 de junio de 2018

70. En la mayoría de los casos, se otorgan reparaciones a las víctimas de la violencia por razón de género, como recursos civiles que incluyen una compensación financiera para sufragar los costos de las pérdidas cuantificables (como la atención médica, la pérdida de salarios y daños materiales), lesiones y pérdidas no cuantificables, además de la necesidad de los supervivientes de reconstruir sus vidas a corto, mediano y largo plazo. Las medidas de reparación también incluyen la eliminación inmediata de los contenidos nocivos, así como formas de restitución, rehabilitación, satisfacción y garantías de no repetición, que combinen medidas simbólicas, materiales, individuales y colectivas, en función de las circunstancias y de las reclamaciones de la víctima. También deberían incluir un requerimiento inmediato a fin de impedir la publicación de contenidos nocivos.

Parlamento Europeo, Resolución de 14 de diciembre de 2021, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia

20. Pide a los Estados miembros que elaboren políticas y programas para apoyar y garantizar la reparación de las víctimas y que adopten medidas adecuadas que eviten que los autores queden impunes, incluida la posibilidad de revisar y modificar su Derecho nacional sobre órdenes judiciales a fin de incluir la ciberviolencia como una de las formas en que puede vulnerarse una orden judicial;

(En el mismo sentido: párr. 43; CDH, 38º periodo de sesiones, "Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales", de 2 de julio de 2018, pág. 6; Relator Especial sobre el derecho a la privacidad, Informe de 24 de marzo de 2020, párrs. 44.c), 45.b.ii y 45.p; ACNUDH, Informe "El derecho a la privacidad en la era digital", de 13 de septiembre de 2021, párr. 61.d).

3. ANEXO: Glosario

ATAQUE DE TROLES (TROLLING)

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, Informe de 18 de junio de 2018

37. El término "ataques de troles" se refiere a la publicación de mensajes, imágenes o vídeos y la creación de etiquetas con el objeto de molestar, provocar o incitar a la violencia contra las mujeres y las niñas. Muchos "troles" son anónimos y usan cuentas falsas para generar el discurso de odio.

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[El] Troleo de género [...] involucra la publicación de contenido extremadamente ofensivo y hashtags en redes sociales para provocar efectos en la opinión pública e incitar a la violencia contra las mujeres. (Pág. 31)

(En el mismo sentido: GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, Anexo).

BODY SHAMING

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] *Body shaming* consiste en comentar y burlarse de la forma, el tamaño o la apariencia corporal de alguien.

CREEPSHOTS

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

La creación y publicación en línea de fotografías o videos de partes íntimas del cuerpo de mujeres y jóvenes registradas mientras éstas se encuentran en espacios públicos [...]. (Pág. 33)

CYBERBULLYNG

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] El ciberbullying es un acoso que se produce a través de herramientas y entornos digitales y que normalmente se entiende que afecta a menores.

CYBERFLASHING

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

Envío de materiales sexualmente explícitos no solicitados [...], incluyendo elaboración y envío de videos de hombres masturbándose o eyaculando con fotografías de la víctima, o de fotografías de penes. (Pág. 31)

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] El *cyberflashing* consiste en enviar imágenes sexuales no solicitadas mediante aplicaciones de citas, aplicaciones de mensajes o textos, o mediante Airdrop o Bluetooth.

DEADNAMING

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] *Deadnaming* es el acto intencional de usar el nombre de nacimiento de una persona trans (que no corresponde a su género) para avergonzar, amenazar, asustar o abusar.

DEEPFAKES

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] Los *deepfakes* son videos en los que una cara ha sido reemplazada (sin problemas) por otra, utilizando algoritmos y aprendizaje profundo, y el sonido se manipula para crear la ilusión de que las acciones de otra persona están siendo escenificadas.

DOWNBLOUSING

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[F]otografías tomadas [...] por arriba de blusas [...]. (Pág. 33)

DOXING

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, Informe de 18 de junio de 2018

36. El término "doxing" alude a la publicación de información privada, como datos de contacto en Internet con intención dolosa, normalmente insinuando que la víctima está ofreciendo servicios sexuales; consiste en investigar y divulgar información de carácter personal sobre una persona sin su consentimiento, a veces con la intención de exponer a una mujer al mundo "real" con fines de acoso y/u otros fines. Incluye situaciones en que la información y los datos personales obtenidos por el autor del abuso se hacen públicos con intención dolosa, en una clara violación del derecho a la intimidad.

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[A]cceso y publicación no autorizada de información personal que revela la identidad de la víctima o su ubicación física, con el objetivo de dañar su reputación, incitar a cometer violencia contra ésta, humillarla, amenazarla o intimidarla o crear daños en su entorno personal, profesional o público, y que genera en muchos casos un contexto de angustia y pánico al propiciar en la víctima miedo sobre su seguridad y la de su familia.

(En el mismo sentido: GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, Anexo).

FLAMING

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] *Flaming* es el acto de publicar mensajes ofensivos u hostiles, incluidos insultos, en redes sociales o foros.

GROOMING

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[A]cción deliberada de un adulto de contactar a una persona menor de edad, a través de medios electrónicos o cualquier otra tecnología de transmisión de datos, con el objeto de ganar su confianza, atacar su integridad sexual o con fines de explotación sexual (incluyendo la obtención, almacenamiento o difusión de pornografía infantil). El *grooming* puede hacerse a través de redes sociales, chats de mensajería instantánea o juegos en línea. (Pág. 36)

INTERNET OF THE THINGS (IOT)

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] IoT es la red de objetos físicos que están conectados entre sí y con Internet, registrando y transmitiendo datos sobre su uso.

ORBITING

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] *Orbiting* consiste en no responder a los mensajes de alguien ni comunicarse directamente con él, sino seguir viendo su contenido en línea (dar me gusta, ver historias, etc.).

OUTING

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

Revelación de la identidad o preferencia sexual de una persona [...], incluyendo exposición de mujeres o integrantes de la comunidad LGTBIQ+ mediante la publicación de sus certificados de nacimiento (Pág. 34)

(En el mismo sentido: GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021, Anexo).

SEALIONING

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[A]coso de una persona con solicitudes persistentes de evidencia, preguntas y/o invitaciones incesantes de involucrarse en un debate en línea con un pretendido sentido de sinceridad y civilidad, a fin de provocar una respuesta agresiva que pueda ser utilizada para contraatacar. (Pág. 31)

SEXTORTION

Consejo de Europa, Comité de la Convención sobre Delitos Cibernéticos, Grupo de Trabajo sobre ciberacoso y otras formas de violencia en línea, especialmente contra mujeres y niños, "Estudio de mapeo sobre ciberviolencia", de 9 de julio de 2018

"Sextorsión" es un término en el discurso popular que abarca actividades que (a) involucran manipulación o coerción para realizar actividades sexuales en beneficio del agresor y/o crear imágenes sexualmente explícitas de la víctima y (b) el delito tradicional de extorsión. Aunque el delito puede incluir la amenaza de difundir dichas imágenes o vídeos una vez creados, es igualmente común que la coerción pueda implicar la amenaza de herir a los familiares o amigos de la víctima si la actividad sexual no se lleva a cabo ni se registra ni se transmite a la víctima. agresor. La motivación del agresor también puede ser la venganza, la humillación o el beneficio económico. A menudo se lleva a cabo de forma remota a través de redes informáticas y puede implicar la grabación de imágenes o la transmisión de vídeo en vivo (es decir, utilizando una cámara web). Los perpetradores suelen ser parejas románticas o sexuales actuales, anteriores o potenciales. Sin embargo, hay casos de "sextorsión" en los que el perpetrador es un extraño y un agresor en serie con víctimas en docenas de países. Los delincuentes suelen utilizar una variedad de habilidades informáticas que incluyen piratería informática, creación de múltiples identidades falsas en sitios de redes sociales, interceptación de comunicaciones privadas, etc. En este sentido, la "sextorsión" ha sido un componente de las formas más graves de ciberacoso y también ha sido un elemento en algunas formas de ciberacoso y ciberacoso. La "sextorsión" a menudo implica la distribución no consensuada de imágenes íntimas, incluso si esa distribución es sólo entre el delincuente y la víctima, en lugar de una difusión amplia. (Pág. 11)

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] La extorsión sexual, también llamada "sextorsión", es el acto de utilizar la amenaza de publicar contenido sexual (imágenes, vídeos, *deepfakes*, rumores sexuales) para amenazar, coaccionar o chantajear a alguien, ya sea para obtener más contenido sexual o dinero, a veces ambos.

(En el mismo sentido: 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, Informe de 18 de junio de 2018, párr. 35).

SWATTING

GREVIO, Recomendación general nº 1 sobre la dimensión digital de la violencia contra las mujeres, de 20 de octubre de 2021

Anexo. [...] *Swatting* es el uso de teléfonos y, a menudo, sistemas informáticos para engañar a un servicio de emergencia y enviar a las autoridades a un lugar específico basándose en un informe falso.

UPSKIRTING

OEA-CIM-MESECVI y ONU Mujeres, Informe "Ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención de Belém do Pará" de 2022

[F]otografías tomadas por debajo de faldas [...]. (Pág. 33)

EUROsocIAL
PROGRAMA PARA LA COHESIÓN SOCIAL
Financiado por la Unión Europea
OEA | MESECVI