ESTUDIO

VIOLENCIA CONTRA MUJERES, NIÑAS, NIÑOS Y ADOLESCENTES EN EL ÁMBITO DIGITAL

El estudio «Violencia contra mujeres, niñas, niños y adolescentes en el ámbito digital» ha sido promovido y financiado por la Delegación del Gobierno contra la Violencia de Género y realizado por la Asociación de Mujeres Juristas Themis.

El objetivo general de esta investigación radica en conocer las peculiaridades de la violencia digital ejercida sobre las mujeres y personas menores de edad y, especialmente, analizar su impacto, así como realizar una aproximación a su regulación normativa. Asimismo, pretende examinar las posibles carencias legales, las dificultades probatorias y el marco normativo existente.

Por consiguiente, los objetivos específicos definidos son los siguientes:

- Análisis de la naturaleza y particularidades de la violencia digital desde una perspectiva de género y de la infancia.
- Conocer los instrumentos normativos para combatir, perseguir y proteger a las víctimas. Principalmente, examinar la legislación española.
- Diagnosticar la influencia del contenido sexual explicito violento y/o inadecuado o violento de cualquier naturaleza en personas menores de edad en relación con la normalización de conductas.
- Evaluar la repercusión de las nuevas tecnologías de la información y de la comunicación en la perpetuación y consolidación de los roles de género, además de valorar la impunidad del agresor en cuanto a la dificultad para perseguir estas actuaciones en el ciberespacio.
- Plantear las reflexiones y apreciaciones de diferentes profesionales implicados en la prevención y persecución de la violencia digital.
- Proponer actuaciones de mejora en la implementación de la normativa y de los mecanismos de protección y detección.

Para abordar los objetivos establecidos, se ha optado por una metodología cualitativa para profundizar en la conceptualización, naturaleza y características de la violencia

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

digital dirigida hacia mujeres y menores de edad. En este estudio se han utilizado dos herramientas: en primer lugar, un análisis exhaustivo de investigaciones, normativas y diversas fuentes bibliográficas; y, en segundo lugar, la realización de un grupo focal con expertos y expertas en la materia. En cuanto a la primera herramienta, se ha realizado un examen detallado del marco normativo y de la codificación de los delitos perpetrados a través de nuevas tecnologías. Asimismo, se han estudiado las nuevas formas de control y dominio ejercidas sobre mujeres y menores en las redes sociales mediante herramientas tecnológicas.

Respecto al grupo focal, se ha celebrado una reunión con profesionales para reflexionar y discutir sobre la violencia digital. Previamente a su celebración, las y los participantes contestaron un formulario de preguntas cerradas, facilitando un debate enriquecedor sobre las perspectivas desde diferentes áreas de especialización. Este proceso ha permitido obtener una visión más completa sobre el alcance de esta forma de violencia y ha sido fundamental para identificar posibles deficiencias y buenas prácticas.

Este estudio se divide en tres grandes bloques: el primer bloque busca un acercamiento a la realidad de la violencia digital; en el segundo, el foco de atención se sitúa sobre las personas menores de edad; y, por último, el tercero, centrado en el marco legislativo. Para concluir, se presentan una serie de conclusiones, propuestas y recomendaciones para mejorar el entorno digital, asegurando que sea saludable y libre de violencias, especialmente hacia las mujeres y las personas menores de edad.

Las principales CONCLUSIONES extraídas de la investigación son las siguientes:

1. Inexistencia de un concepto único y universal de «violencia digital». Esto dificulta una normativa uniforme en cuanto a su naturaleza, tipología, características, así como a su regulación penal.

   No obstante, sí existen referencias a la violencia digital en diferentes textos normativos y documentos a nivel europeo y estatal. Algunos ejemplos son: la definición de ciberviolencia del Consejo de Europa, que la describe como: «*el uso de sistemas informáticos para causar, facilitar o amenazar con violencia contra las personas, que tiene como resultado, o puede tener como resultado, un daño o sufrimiento físico, sexual, psicológico o económico, y puede incluir la explotación de la identidad de la persona, así como de las circunstancias, características o vulnerabilidades de la persona*» o el concepto introducido por la Relatora Especial sobre la Violencia contra las Mujeres que la delimita como: «*todo acto de violencia por razón de género contra la mujer cometido, con la asistencia, en parte o en su totalidad, del uso de las TIC, o agravado por este, como los teléfonos móviles y los teléfonos inteligentes, Internet, plataformas de medios sociales o correo electrónico, dirigida contra una mujer porque es mujer o que la afecta en forma desproporcionada*».

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

En España, las primeras nociones se encuentran en la Ley Orgánica 8/2021 de protección integral de la infancia y la adolescencia frente a la violencia y en la Ley Orgánica 10/2022 de protección integral de la libertad sexual. Aunque estas normas se limitan a realizar una enumeración de actos que pueden construir el concepto, sin llegar a definirlo.

Por último, la Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, de 14 de mayo de 2024, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, y que tiene por objeto esencial, desde el punto de vista del derecho sustantivo, proporcionar las líneas maestras para que se produzca la armonización de las normas penales en materia de ciberviolencia, no recoge un concepto de violencia digital de género. Sin embargo, el texto de la Propuesta de Directiva sí lo establecía, por ello, se ha perdido una oportunidad de ofrecer una definición única para el territorio de la Unión Europea, lo que facilitaría el desarrollo de las normativas comunes en la materia.

2. Las estadísticas de diversas investigaciones muestran que la violencia digital impacta principalmente en mujeres y niñas. Esta forma de violencia es una continuación de la que ocurre en el mundo físico, arraigada en estructuras patriarcales y roles de género que, en lugar de desvanecerse, se replican en el entorno virtual. Entre los datos más relevantes destacan: la investigación de la ONU «Combatir la violencia en línea contra las mujeres y niñas: Una llamada de atención al mundo», que señala que más del 73 % de las mujeres de ámbito mundial han sido expuestas o han experimentado algún tipo de violencia en internet y el 90 % de las víctimas de distribución de imágenes íntimas de contenido sexual sin consentimiento son mujeres. Igualmente, en la Encuesta Europea de Violencia de Género, elaborada por la Delegación del Gobierno contra la Violencia de Género, muestra que han experimentado acoso de manera reiterada un 30,6 % de las mujeres de entre 16 y 17 años y un 33 % entre los 18 y 29, siendo los agresores hombres en un 85,8 % de los casos. Y el Informe sobre delitos contra la libertad sexual del Ministerio del Interior de 2023 indica que el 66 % de las victimizaciones registradas por ciberdelincuencia sexual son mujeres, mientras que el 96 % de los ciberdelincuentes sexuales investigados o detenidos son hombres.

   La ausencia de datos estadísticos que estudien la ciberviolencia con unos parámetros comunes y uniformes es significativa, dificultando así la extracción de información esencial para la evaluación del alcance de este tipo de violencia. Esto implica, por ejemplo, que la definición de ciberviolencia y su regulación penal varíen dependiendo de quién elabore la estadística.

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

Destacar que, en general, existe una falta de conexión entre los diferentes tipos de delitos, lo que lleva a que los casos de ciberviolencia se clasifiquen bajo delitos más graves sin considerar el medio y origen tecnológico del delito inicial. Esta falta de información obstaculiza la comprensión de la ciberdelincuencia, impidiendo una cuantificación y análisis adecuados de los ciberdelitos de género, lo que a su vez complica la implementación de medidas efectivas al respecto.

Por otro lado, reseñar que las últimas investigaciones y estadísticas evidencian que cada vez se accede a edades más tempranas a la pornografía a través de los primeros dispositivos electrónicos. Las personas menores de edad son nativos digitales que navegan en un entorno con insuficientes barreras de protección y a nivel cerebral no están preparadas para el impacto de este tipo de contenido. El porno se convierte en una fuente de aprendizaje para la juventud, normalizando y perpetuando una violencia estructural hacia las mujeres, al objetivarlas y deshumanizarlas.

De igual modo, se lleva a cabo una breve reflexión sobre los efectos nocivos del consumo de pornografía en personas menores de edad. La Agencia Española de Protección de Datos, la ONG «Dale una vuelta» y la Fundación del Colegio Oficial de Psicología de Madrid han incorporado en su trabajo *El impacto de la pornografía en menores* algunas de las graves consecuencias derivadas de este consumo. Entre ellas, destacan problemas de rendimiento académico, el deterioro en la capacidad de atención, memoria procedimental (que permite almacenar habilidades, procedimientos y destrezas motoras o cognitivas) y en la capacidad de organización y planificación. Igualmente, advierten que el consumo ocasional de pornografía puede conducir a un comportamiento adictivo en menores de edad y adolescentes.

3. El uso de las tecnologías de la información y la comunicación (TIC) ha sido clave para empoderar a las mujeres y sus comunidades. Estas herramientas se han convertido en un recurso fundamental para organizar la acción colectiva feminista, dar visibilidad a discursos de concienciación y reivindicación social a gran escala y aumentar la capacidad de convocatoria, superando las barreras físicas que presenta el ámbito analógico.

   A nivel internacional, movimientos como el «*Me Too*» han permitido que mujeres de diferentes sectores y lugares del mundo compartan sus experiencias de violencia sexual, generando un importante debate sobre el acoso y abuso en la industria del cine, la música, la ciencia y la política. En España, las redes sociales han sido un motor para movilizar a la sociedad sobre diversas problemáticas relacionadas con la violencia de género y la defensa de los derechos de las mujeres. Por ejemplo, el movimiento

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

«Ni Una Menos» se ha enfocado en visibilizar los asesinatos machistas, mientras que el «Tren de la Libertad» ha luchado por los derechos sexuales y reproductivos. Además, el movimiento social feminista en el marco del Día Internacional de la Mujer del 2018 movilizó a miles de mujeres en la primera huelga feminista, convirtiéndose en un hito histórico en nuestro país. La campaña «Yo sí te creo, hermana» se difundió rápidamente en las redes, donde muchas mujeres compartieron sus testimonios y experiencias, organizando concentraciones y protestas en toda España para exigir un cambio significativo en la manera en que la sociedad y las instituciones abordan los delitos sexuales. Posteriormente, gracias a las redes sociales el movimiento feminista volvió a la calle bajo el lema «Se acabó», tras el caso del beso no consentido del presidente de la Real Federación Española de Fútbol, siendo contundente la condena social.

4. En los últimos años, el avance de la Inteligencia Artificial (IA) ha sido exponencial y ha generado nuevos retos y peligros que deben ser afrontados por las instituciones y el derecho. Es importante explicar que el funcionamiento de la IA implica que ésta almacena y examina un elevado número de datos para instruirse y realizar tareas de manera autónoma; por lo que, si esos datos contienen errores o prejuicios, serán replicados por la IA suscitando la presencia de sesgos de género y discriminación, vulneración de seguridad y privacidad, ausencia de controles y falta de transparencia. Esto puede llevar a decisiones injustas en áreas como la contratación, la justicia penal y el acceso a servicios.

   Por ello, la Unión Europea comenzó a elaborar varias propuestas para dar respuesta a la necesidad de establecer límites y controles en aras a la protección de nuestros derechos y garantías. Estos trabajos concluyen en marzo de 2024 con la primera normativa europea sobre IA. La norma establece límites en el uso de la identificación biométrica, así como, la prohíbe para manipular o explotar las vulnerabilidades del usuario y otorgar derechos a los y las consumidoras para presentar quejas y recibir explicaciones. Uno de los objetivos principales de esta regulación es garantizar la protección de los derechos fundamentales de las personas, al mismo tiempo que fomentar la innovación y posicionar a UE como líder en este ámbito.

5. Las personas menores de edad son particularmente susceptibles a los peligros asociados con la interacción en línea. La exposición a contenido inapropiado, el fácil acceso a redes sociales y la falta de una supervisión adecuada fomentan la normalización de comportamientos inadecuados y la victimización. La inmadurez y

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

la falta de pensamiento crítico en la infancia y adolescencia, junto con una educación digital insuficiente, los hacen más vulnerables a la explotación por parte de depredadores en línea, enfrentándose a amenazas como el *grooming*, el ciberacoso y la explotación sexual digital. Además, el acceso sin restricciones a redes sociales y las aplicaciones de mensajería instantánea ha facilitado que los agresores ejerzan un control invasivo y lleven a cabo diversas formas de ciberviolencia, incluyendo ciberacoso, sextorsión y explotación sexual en línea.

6. La ciberviolencia es un fenómeno criminal muy dinámico y en continua transformación, cuyas repercusiones impactan a toda la sociedad y, en particular, a las mujeres. Esto lleva a los legisladores a estar en constante búsqueda de soluciones para las nuevas problemáticas surgidas por el avance tecnológico, ajustando las leyes a la realidad social actual. En este sentido, España destaca como un país avanzado en la regulación penal.

   En los últimos años, en cuanto al entorno digital, la legislación española se ha ido adaptando a las necesidades en materia penal y procesal para intentar dar una respuesta adecuada a la defensa de la tutela judicial efectiva de los derechos de las mujeres y de las personas menores de edad. Para ello, se ha reformado el Código Penal y la Ley de Enjuiciamiento Criminal, así como se han promulgado nueva normativa.

   En el estudio se han analizado las principales reformas. En 2010, se aprueba la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre. Esta norma tipifica nuevas conductas en el ámbito de la prostitución y de la pornografía infantil. Por ejemplo, se añade el artículo 183 bis para regular la práctica conocida internacionalmente como «*child grooming*» y establece que aquel que, a través de Internet, teléfono u otra tecnología de la información y la comunicación, contacte a un o una menor de trece años y proponga encontrarse con él para cometer ciertos delitos (descritos en los artículos 178 a 183 y 189) será castigado con prisión de uno a tres años o multa de doce a veinticuatro meses, siempre y cuando haya actos materiales que busquen acercarse al menor. Las penas serán más severas cuando el acercamiento a un menor se realice mediante coacción, intimidación o engaño. Además, se suprime el apartado 8 del artículo 189 del Código Penal y se modifica el primer párrafo, las letras a) y b) del apartado 1 y el primer párrafo del apartado 3 de este precepto 189. Por ende, se incluye la captación de menores para participar en espectáculos pornográficos y se aborda la conducta de aquellos que obtienen beneficios económicos de la participación de menores en este tipo de espectáculos.

   Posteriormente, se aprueban la Ley Orgánica 1/2015, de 30 de marzo, por la que modifica la Ley Orgánica 10/1995, de 23 de noviembre y la Ley Orgánica 13/2015, de 5 de octubre,

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

Para completar la protección de las personas menores frente a los abusos cometidos mediante el uso de Internet u otras telecomunicaciones, en la Ley Orgánica 1/2015 se introduce el artículo 183 ter para sancionar al que a través de medios tecnológicos contacte con un o una menor de quince años y realice actos dirigidos a embaucarle para que le facilite material pornográfico o le muestre imágenes pornográficas, siendo el antecedente normativo más directo del artículo 183 ter 1º Código Penal (antiguo artículo 183 bis). La reforma del año 2015 ha conservado en gran parte el contenido del articulado original introducido por la modificación de 2010.

Uno de los cambios más significativas de la Ley Orgánica 1/2015 fue elevar la edad del sujeto pasivo de 13 a 16 años. Además, estableció que el sujeto activo debe tener como objetivo llevar a cabo, ya sea cometer un abuso o una agresión sexual contra menores de dieciséis años, o su uso con propósitos exhibicionistas o pornográficos, tal como se contemplaba en los artículos 183 y 189 del Código Penal, suprimiéndose así la remisión a los arts. 178, 179, 180, 181 y 182 de este Código.

Al mismo tiempo, se tipifica en el artículo 197.7 del CP como nuevo delito (*sexting* de tercero) la divulgación no autorizada de grabaciones o imágenes íntimas obtenidas con el consentimiento de la víctima, pero luego divulgados sin que esta lo permita, cuando afecten gravemente a su intimidad.

Igualmente, se estructura un nuevo delito de acoso, acecho u hostigamiento (*stalking*) en el artículo 172 ter para dar cumplimiento al artículo 34 del Convenio de Estambul. Regula aquellos supuestos en los que, sin llegar a producirse necesariamente el anuncio explícito o no de la intención de causar algún mal (amenazas) o el empleo directo de violencia para coartar la libertad de la víctima (coacciones), se producen conductas reiteradas por medio de las cuales se menoscaba gravemente la libertad y sentimiento de seguridad de la víctima, a la que se somete a persecuciones o vigilancias constantes, llamadas reiteradas, u otros actos continuos de hostigamiento.

Finalmente, la Ley Orgánica 1/2015 añade al artículo 189 del CP el nuevo apartado 8, el cual otorga a jueces y tribunales la autoridad para ordenar la eliminación de páginas web o aplicaciones de Internet que contengan o difundan pornografía infantil, así como aquellas que hayan sido creadas utilizando a personas con discapacidad que requieren una protección especial.

En otro orden de cosas, la reforma de la Ley 13/2015 incluyó la incorporación de nuevas disposiciones en la Ley de Enjuiciamiento Criminal, que facilitan las herramientas de investigación en el ámbito digital. Entre ellas, destaca: el artículo 588 Octies, que

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

regula la preservación de datos informáticos (artículo 16 del Convenio de Budapest); los artículos 588 ter j) y siguientes, que se refieren a la solicitud de datos almacenados a terceros (artículo 18 del Convenio de Budapest), y los artículos 588 Sexies a), b) y c), que abordan el registro de dispositivos informáticos (artículo 19 del Convenio de Budapest).

Hasta la aprobación de la Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia no se produce ninguna modificación sustantiva. Esta norma introduce nuevos tipos delictivos en el Código Penal para evitar la impunidad de conductas realizadas a través de medios tecnológicos y de la comunicación, que producen graves riesgos para la vida y la integridad de las personas menores de edad, así como una gran alarma social. Así, la distribución o difusión pública a través de Internet, teléfono u otras tecnologías de contenidos destinadas a promover, fomentar o incitar al suicidio de personas menores de edad o con discapacidad necesitadas de especial protección será castigada con pena de prisión de uno a cuatro años (artículo 143 bis) y la distribución o difusión pública a través de Internet, teléfono u otras tecnologías de contenidos destinados a promover, fomentar o incitar a la autolesión de personas menores de edad o con discapacidad necesitadas de especial protección será castigada con pena de prisión de seis meses a tres años (artículo 156 ter). Además, se prevé expresamente la retirada de estos contenidos por las autoridades judiciales para evitar la persistencia delictiva.

De igual modo, se modifica nuevamente el artículo 189 en las letras b), c) y g) del apartado segundo. El artículo busca penalizar el uso y la distribución de material pornográfico que involucre a menores de edad o personas con discapacidad. Las letras b), c) y g) disponen aplicar una pena mayor en determinados supuestos: cuando los hechos son particularmente degradantes o vejatorios, o cuando se emplea violencia física o sexual para obtener dicho material, o se representan escenas de violencia física o sexual, cuando se utilizan personas menores de edad que se encuentran en una situación de especial vulnerabilidad debido a enfermedad, discapacidad u otras circunstancias y cuando el responsable del delito de pornografía infantil es un ascendente, tutor, curador, guardador, maestro u otra persona encargada de la persona menor de edad o persona con discapacidad necesitada de especial protección. Y la pena se agrava si la persona que cometió el delito convive con el menor de edad o la persona con discapacidad, o si ha abusado de su posición de confianza o autoridad para cometer el delito.

En los últimos años, es preciso mencionar la La Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la Libertad Sexual (LOGILS). En concreto, se añade un apartado 5 al artículo 172 ter del Código Penal (CP), que tipifica el hecho de usurpar la identidad de otra persona en redes sociales y causarle con ello acoso, hostigamiento

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

o humillación. Y también un párrafo 2 al artículo 197.7 del CP, que sanciona a quien, habiendo recibido las imágenes o grabaciones audiovisuales, obtenidas con el consentimiento de la persona afectada en un lugar privado sin presencia de terceras personas, las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada. El legislador pretendía imponer el castigo a los terceros, pero es una cuestión controvertida y, por ahora, la jurisprudencia es limitada.

Adicionalmente, la LOGILS introduce un párrafo segundo en el artículo 13 de la Ley de Enjuiciamiento Criminal, que establece la posibilidad de solicitar la adopción de medidas cautelares dirigidas de forma específica a la delincuencia sexual *online*. También, se da una nueva redacción al precepto 681.3, que remite al artículo 3 de la LOGILS. Con ello, añade a la relación de víctimas respecto de las que no se puede difundir su identidad a aquellas víctimas de los delitos contra la libertad sexual, de mutilación genital, matrimonio forzado y trata con fines de explotación sexual, lo que era una exigencia de adición para completar más su protección en base a la filosofía del texto de la Ley. Y destaca, de esta reforma, que amplía la lucha contra la delincuencia sexual *online* que tanto daño está haciendo en la actualidad, sobre todo en el caso de víctimas menores, por conductas de quienes se hacen pasar en línea por un menor de edad también para conseguir sus fines perversos.

En 2023, se ratifica la Ley Orgánica 1/2023, de 28 de febrero, por la que se modifica la Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo. Esta norma introduce una agravación en relación con el apartado 5 del artículo 172 ter, cuando la víctima sea menor o persona con discapacidad, en cuyo caso se aplicará la pena en su mitad superior.

Por último, en el tiempo actual está en trámite el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, que pretende responder a la necesidad de crear un entorno digital más seguro para las personas menores de edad y adolescentes, protegiéndolas de los peligros identificados por expertos científicos, educativos y organizaciones dedicadas a la protección de la infancia y la juventud.

En la parte jurídica del anteproyecto, se propone la tipificación de nuevos delitos, que castigan acciones como las conocidas como *deepfakes* o ultrafalsificaciones. Estas consisten en la difusión, exhibición o cesión sin consentimiento de imágenes y audios creados a través de inteligencia artificial o tecnologías avanzadas, y que tienen un contenido altamente realista, siempre que los hechos que representen sean gravemente vejatorios o de contenido sexual. Además, se establece un tipo agravado para el caso de que la acción se difunda en el ciberespacio, cuando sea posible que alcance a un número indeterminado de personas.

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

Junto a ello, se incluyen sanciones para las personas adultas que elaboran un perfil falso de edad y/o género para entablar contacto con menores mediante el engaño *online* con la finalidad de cometer un delito contra la libertad sexual.

De igual manera, se establecen limitaciones a las empresas tecnológicas, ya que los fabricantes deberán garantizar que los dispositivos cuentan con sistemas de control parental y etiquetado informativo sobre el impacto negativo de los dispositivos digitales. A su vez, las plataformas de intercambio de vídeos, deberán incluir un enlace directo, visible y de fácil acceso al canal de denuncias y al control parental, eliminando la dificultad a los progenitores en esta labor de denuncia. Además, atendiendo al carácter adictivo de las recompensas asociadas con videojuegos y plataformas digitales, denominadas «*loot boxes*», se regula la prohibición de acceso de los y las menores a las mismas.

Por otro lado, se reforzarán las obligaciones a los *influencers* o creadores de contenido masivo en su actividad para que adopten en sus publicaciones medidas de protección adecuadas para los y las menores.

7. En el delito de trata de mujeres y niñas con fines de explotación sexual, las TIC han favorecido la captación, ofrecimiento y control de las víctimas, con menores riesgos y mayores beneficios. Debemos de tener en cuenta que los métodos utilizados por las organizaciones criminales van perfeccionándose progresivamente, cada vez utilizan más instrumentos *online* a través de páginas web y redes sociales. No hay que ignorar cómo la tecnología favorece el proceso de traslado de la víctima de un país a otro mediante el uso de técnicas de ocultación del rastreo o, por ejemplo, entorpeciendo la vinculación entre autores y víctimas a través de sistemas de anonimización de identificación digital.

8. La naturaleza transfronteriza de la ciberdelincuencia requiere una cooperación internacional efectiva. El Informe de Impacto que acompaña a la Propuesta de Reglamento *E-Evidence* de la Comisión Europea revela que cada vez en mayor número de investigaciones se requiere de una solicitud transfronteriza de acceso a pruebas electrónicas. El 85 % de los casos precisan datos digitales y es necesario reclamar pruebas a proveedores de servicios en línea con sede en otra jurisdicción en dos tercios de las investigaciones. Por ello, para mejorar este acceso transfronterizo a las pruebas electrónicas, en 2019 la Comisión Europea propuso iniciar negociaciones internacionales para favorecer la localización de los delincuentes y simplificar los mecanismos. La Comisión entabló dos vías de negociación: una con Estados Unidos,

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

que se encuentra en curso, y otra para la elaboración del Segundo Protocolo Adicional al Convenio de Budapest. Con respecto a la primera, mencionar que, en la actualidad, los proveedores de servicios con sede en EE.UU. colaboran voluntariamente con las autoridades policiales europeas. Sin embargo, la legislación estadounidense no siempre permite que los datos solicitados sean proporcionados directamente a las autoridades europeas en respuesta a solicitudes de acceso. En relación a la segunda vía, en lo que respecta al Segundo Protocolo, pretende fortalecer la cooperación entre las autoridades de los diferentes países en la lucha contra la ciberdelincuencia, así como garantizar la eficaz obtención y revelación de las pruebas electrónicas.

Por lo expuesto, cabe remarcar que la rápida evolución de la tecnología y la creciente importancia de la evidencia digital en los casos judiciales plantean desafíos para el sistema judicial. Ante esta situación, en muchos casos, los y las profesionales de la judicatura y de la abogacía carecen de la especialización en temas digitales y tecnológicos. La falta de conocimiento especializado en temas digitales puede dificultar la comprensión de la evidencia digital presentada, así como la evaluación de la validez y confiabilidad de dicha evidencia. La dificultad para comprender los aspectos técnicos y forenses puede llevar a decisiones erróneas o a una falta de apreciación adecuada de la importancia de dicha evidencia en el caso. A diferencia de lo que ocurre en la Fiscalía, que sí ha implementado salas especializadas de criminalidad informática, la judicatura no se ha especializado. En consecuencia, la formación especializada en esta materia es prioritaria.

9. La falta de formación especializada desde la perspectiva de género en el ámbito de la ciberdelincuencia y la insuficiencia de recursos materiales y personales representan obstáculos significativos en la lucha contra la violencia digital que afecta a mujeres y a las personas menores de edad. La escasez de capacitación adecuada en ciberseguridad y en el manejo de la violencia digital desde una perspectiva de género limita la capacidad de los profesionales y las profesionales de la educación, la salud, el trabajo social y las fuerzas de seguridad para identificar, prevenir y responder eficazmente a estos delitos. Además, la carencia de medios específicos destinados a la implementación de programas de apoyo y plataformas seguras para las víctimas, agrava la situación dejándolas sin la protección y el apoyo necesarios. Esta brecha formativa y de recursos perpetúa la vulnerabilidad de las mujeres y las niñas en el entorno digital y subraya la urgente necesidad de invertir tanto en formación especializada como en la dotación de medios adecuados para un abordaje integral de la violencia digital.

10. Las devastadoras consecuencias de la violencia digital para las víctimas es alarmante, puesto que se produce una amplificación notoria sobre los bienes jurídicos afectados: honor, intimidad, dignidad, libertad o integridad moral. La situación de

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

conectividad permanente, unida con la rapidez y capacidad de difusión, hacen que la lesión se permanezca en el tiempo y alcance a un gran número de personas. En idéntico sentido, secuelas relacionadas con la disminución de la autoestima, ansiedad, depresión y, en casos extremos, pensamientos suicidas. La violencia digital aumenta la vulnerabilidad de las mujeres y personas menores de edad, perpetúa las desigualdades de género existentes y creando nuevas formas de victimización en el espacio digital.

La transformación digital es un proceso en constante evolución que implica afrontar nuevos retos para crear un entorno en línea seguro, predecible y digno de confianza. Ante lo expuesto, en el estudio se plantean una serie de PROPUESTAS:

1.

Se enuncia como posible definición universal de «violencia digital» la siguiente:

> «Todos aquellos actos delictivos que, por razones de discriminación de género, afecten negativamente a las mujeres y a las niñas, utilizando el entorno tecnológico y/o producidos en el mundo digital».

2.

Ante los datos mostrados, la implementación de medidas para la prevención de la violencia de género en el ámbito digital requiere de un abordaje integral de forma imperiosa. Esto implica la promoción de la educación y de la concienciación sobre el uso responsable de las tecnologías, así como el fomento de una cultura de respeto y equidad de género en línea.

3.

Medidas de sensibilización, concienciación, prevención y detección: se recomienda el desarrollo de campañas específicas con perspectiva de género y de infancia diseñadas para sensibilizar, concienciar, prevenir y detectar sobre los posibles riesgos y delitos de la violencia digital. Estas iniciativas serían eficaces siempre y cuando se cuente con normativa y políticas públicas que pongan el foco en la protección de las víctimas y en la sanción a los agresores, así como brindarles el apoyo y los recursos adecuados para superar las consecuencias de este tipo de violencia.

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

4.

Atención y asesoramiento especializado e integral: la atención y el asesoramiento especializado e integral a las víctimas en todas las fases del procedimiento judicial es una medida urgente a adoptar. Esta orientación no debe limitarse sólo al ámbito jurídico, sino que también debe abarcar el psicológico. El acompañamiento psicológico debe llevarse a cabo desde el inicio del proceso para fomentar la recuperación y evitar lesiones psicológicas irreversibles, al mismo tiempo que se configura como un apoyo esencial para enfrentarse a las consecuencias del proceso penal.

5.

Formación especializada y multidisciplinar con enfoque de género: la formación de todos los y las profesionales intervinientes en los procesos por casos de violencia digital (fuerzas y cuerpos de seguridad, abogacía, judicatura, equipos psicosociales adscritos a los juzgados, etc.) con el fin de facilitar la persecución, imputación y sanción de los delitos tecnológicos; y, los programas de formación permitirían una mejor atención a las víctimas y la reparación del daño.

6.

Protocolos unificados de atención: la creación de protocolos específicos unificados y adaptados a la violencia digital en todos los ámbitos, incluyendo el educativo, sanitario, judicial y policial con objeto de garantizar la coordinación de servicios que permita garantizar la protección de las víctimas.

7.

Delito de usurpación de identidad digital: se recomienda tipificar un delito de usurpación de identidad digital, ya que en nuestro ordenamiento jurídico no existe una respuesta penal adecuada, con independencia de la posibilidad de resolver estas situaciones en la jurisdicción administrativa o, civil. Actualmente nuestro CP se limita a sancionar la creación de perfiles falsos o apertura de anuncios, ocasionando con ello a la víctima una situación de acoso, hostigamiento o humillación (art. 172 ter.5). Sin embargo, la suplantación no siempre se restringe a estos comportamientos, de ahí la necesidad de su tipificación.

El uso intencionado de los datos personales de una persona identificable, ya sea en la totalidad o en gran parte, de sus interacciones en línea, con efectos duraderos y con características que le otorguen credibilidad, puede llevar a confusiones sobre la

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

participación de la persona suplantada en esos medios. Esta conducta representa una grave violación de la privacidad y puede afectar de manera significativa a las relaciones de la víctima con otras personas.

8.

Profesionales en informática forense y extracción de evidencia digital: se precisa de personal profesional en informática forense, ya que la recolección de evidencia digital es un proceso delicado que requiere de expertas y de expertos cualificados en la identificación, recolección, análisis y preservación de la evidencia digital. Este personal experto en ciencia forense digital debe formar parte de los equipos de las fuerzas y cuerpos de seguridad como de los tribunales y juzgados, dada la naturaleza y características de la prueba digital.

9.

Importancia del conocimiento de datos estadísticos: la estadística es una herramienta indispensable para tener una aproximación real de la naturaleza y de las características de la problemática de la ciberviolencia. Los datos estadísticos tienen un papel esencial en la generación de conocimiento y la toma de decisiones. En este sentido, se manifiesta la necesidad de la elaboración de una clasificación estadística propia y que esté interrelacionada con aquellos delitos perpetrados fuera de la espera virtual y que tienen su origen en el ámbito digital. Del mismo modo, es fundamental que los datos estadísticos estén disgregados por sexo para así determinar el alcance real de la ciberviolencia hacia las mujeres y las personas menores de edad.

10.

En el acceso de las personas menores de edad a contenidos pornográficos desempeña un papel clave el grado de implicación de las instituciones educativas y de las familias en la educación afectivo-sexual con el fin de contribuir al crecimiento integral personal y emocional. El Estado debe implementar acciones específicas encaminadas a impedir el acceso de menores a la pornografía en internet, puesto que la pornografía dificulta el desarrollo de una sexualidad saludable en la adolescencia y la infancia, promueve prácticas agresivas y denigratorias y limita la capacidad de establecer relaciones sanas basadas en el respeto mutuo, el consentimiento y el placer compartido.

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

11.

Programas de buenas prácticas de las TIC: el desarrollo de estratégicas y acciones de protección específica de los datos de menores almacenados en Internet. La implementación de medidas de mejora en la alfabetización mediática, incidiendo especialmente en una educación que integre una seguridad en la Red que pueda servir como mecanismo de prevención de lucha contra las amenazas del mundo online. Asimismo, la instauración de programas de buenas prácticas de las TIC para progenitores y para menores y estableciendo como obligatorios o muy recomendables los mecanismos de control parental en los dispositivos electrónicos con objeto de bloquear el contenido violento y/o sexual inadecuado para su edad.

12.

Colaboración institucional: la colaboración entre los gobiernos, las autoridades y las organizaciones civiles debe ser activa y permanente para identificar nuevas formas de explotación en línea. Estas alianzas también permitirán articular estrategias de prevención y lucha contra la trata de personas, especialmente con fines de explotación sexual, en los entornos digitales.

13.

Políticas uso responsable de la Inteligencia Artificia: El desarrollo de la IA exige la implementación de políticas y de normativas idóneas que garanticen un uso ético y seguro. En este sentido, habrá que estar permanecer atentas al grado de cumplimiento de las directrices establecidas en la primera normativa europea de IA.

14.

Tipificación nuevo delito: Es necesario tipificar como nuevo delito contra la integridad moral aquellos supuestos en los que una persona se apropie de una imagen o vídeo o ficheros de voz, con o sin consentimiento, y los manipule sin consentimiento mediante sistemas automatizados, software, algoritmos o inteligencia artificial para la difusión pública de su imagen corporal o audio de voz con la intención de menoscabar su integridad moral, honor, dignidad o la propia imagen, creando a través de la simulación situaciones de apariencia real. Este nuevo delito también castigará a la persona que, habiendo recibido la imagen o grabación manipulada, contribuya a su difusión, revelación o cesión a terceros. Quizás este tipo de conductas queden contempladas en el nuevo artículo 173 bis del Anteproyecto de Ley Orgánica para la protección de personas menores de edad en los entornos digitales.

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es

15.

La información y la formación sobre los diversos peligros de las redes sociales y de las nuevas tecnologías deben centrarse en los mecanismos de protección, control, identificación y detección de riesgos para así generar autoprotección.

16.

Formación transversal y obligatoria: La formación transversal y obligatoria con perspectiva de género digital es indispensable para que las familias, las personas menores de edad y los diversos profesionales tengan conocimientos actualizados.

Alcalá, 37
28014 Madrid
prevencionyestudiosvg@igualdad.gob.es