ESTUDIO

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

Themis
Asociación de Mujeres Juristas

MINISTERIO DE IGUALDAD

SECRETARÍA DE ESTADO DE IGUALDAD Y PARA LA ERRADICACIÓN DE LA VIOLENCIA CONTRA LAS MUJERES

DELEGACIÓN DEL GOBIERNO CONTRA LA VIOLENCIA DE GÉNERO

Este estudio ha sido promovido y coordinado por la Delegación del Gobierno contra la Violencia de Género, realizado por la Asociación de Mujeres Juristas Themis.

NIPO en línea: 048-25-018-3

Correo electrónico: dgviolenciagenero@igualdad.gob.es

Catálogo de Publicaciones de la Administración General del Estado: https://cpage.mpr.gob.es

Autoras:

Laura Fernández Gómez, Paz Lloria García,
Cristina Ventura Alameda, Mercedes Yela Uceda.

Revisión de contenido:

Paz Lloria García

Revisión de estilo:

Mónica Casás Díaz

AGRADECIMIENTOS

Quisiéramos expresar nuestro agradecimiento especial a Paz Lloria García por su inestimable ayuda como correctora de contenido, aportando claridad y precisión al texto, así como por sus comentarios y sugerencias que, indudablemente, han enriquecido notablemente la investigación.

De igual modo, nuestro más sincero agradecimiento a todas y cada una de las expertas que participaron en el encuentro profesional de este estudio, por su interés, el tiempo y esfuerzo dedicados, así como por sus valiosas ideas e intercambio de experiencias desde su especialización en la materia, contribuyendo al enriquecimiento de la dinámica de grupo y al éxito del taller. Gracias a Mar España Martí (directora de la Agencia Española de Protección de Datos), a Myriam Hernández Marcos (fiscal adscrita a la Unidad de Criminalidad Informática), a Silvia Barrera Ibáñez (jefa de Grupo de Delitos Tecnológicos de La Rioja de la Policía Nacional), a José Moratalla Alfaro (agente de policía local del Grupo GAMA de Valencia) y a Ruth Sala Ordóñez (abogada penalista, especialista en delitos informáticos y prueba digital).

ÍNDICE

INTRODUCCIÓN

1. JUSTIFICACIÓN

En los últimos años, el uso de dispositivos electrónicos y nuevas tecnologías de la información y comunicación (TIC) es uno de los factores que más cambios ha producido en la sociedad, haciéndose imprescindible su uso en la vida cotidiana de las personas. Según el *Estudio anual de Redes Sociales 2023*, aproximadamente treinta millones de individuos de entre 12 y 74 años utilizan redes sociales (85 %), especialmente las personas jóvenes de 18 a 24 años (94 %)[1].

El fenómeno no es nuevo. El manejo y consolidación de Internet como una red mundial de información y comunicación comienza a tener importancia en la década de los años noventa. Además, la aparición de dispositivos móviles (teléfonos inteligentes o *smartphones*, *tablets*, *etc.*) y de los servicios de mensajería instantánea (*Messenger*, *Line*, *Skype*, *WhatsApp*, *Telegram*, *Facebook Messenger*, *Instagram*) supuso una revolución en la comunicación social, convirtiéndose en la actualidad en un instrumento indispensable en el día a día, en su vertiente más amplia, ya que se han consolidado como instrumentos de trabajo y de relación social.

El uso masivo de las tecnologías sufrió un cambio cualitativo durante la pandemia por COVID-19. La situación de aislamiento y confinamiento domiciliario obligó a articular y a normalizar, precipitadamente, mecanismos de teletrabajo e informatización de todo tipo de prestaciones, como modo de permitir el acceso a todos los servicios, gestiones y actividades. La población tuvo que adaptarse a este nuevo escenario, en algunos casos, sin tener ningún conocimiento previo sobre el uso de las TIC.

En tiempo récord se ha originado un gran avance en todos los sentidos, puesto que conlleva la interconexión entre países, el acceso al conocimiento, ser altavoz de reivindicaciones y la visibilización de realidades sociales, políticas, bélicas, culturales, comerciales, etc. Esta digitalización ha facilitado innumerables actividades, ya que se abre todo un mundo de posibilidades haciendo un simple «*clic*». Sin embargo, a su vez, entraña una serie de peligros, amenazas de seguridad y privacidad para los y las usuarias de la era digital. El lado más oscuro de las TIC puede suponer la comisión de nuevos tipos delictivos que conviven con los tradicionales.

En relación con la violencia machista, el uso de las redes sociales y las aplicaciones de mensajería instantánea ha facilitado que los agresores puedan ejercer un control aún más invasivo sobre sus parejas, puesto que pueden monitorear constantemente sus actividades en línea, acosarlas o difundir información privada de forma rápida y masiva.

Fuera del ámbito de la pareja, también se han observado formas de violencia de género relacionadas con las nuevas tecnologías. Basta citar algunos ejemplos de ciberviolencia, como son el *ciberbullying*, el *grooming*, la *sextorsión* o el *trolling*. Otras formas delictivas tradicionales han adoptado manifestaciones

[1] IAB. *Estudio de Redes Sociales*, 2023, pp. 11. Disponible en: https://iabspain.es/estudio/estudio-de-redes-sociales-2023/

tecnológicas, como la explotación sexual en línea o la prostitución, así como la trata de personas con fines de explotación sexual, que pueden tener graves consecuencias para las víctimas, como la disminución de la autoestima, ansiedad, depresión e, incluso, pensamientos suicidas.

Esta situación ha sido referenciada en *La Estrategia de la UE sobre los derechos de las víctimas* (2020-2025), donde se señala que:

> *«Una parte cada vez más importante de nuestras vidas se produce en línea, una tendencia que se ha acentuado aún más durante la pandemia de COVID-19. La ciberdelincuencia puede consistir en delitos graves contra las personas, como los delitos sexuales en línea (incluidos los delitos contra los menores), la usurpación de identidad, los delitos de odio en línea y los delitos contra la propiedad (como el fraude y la falsificación de medios de pago distintos del efectivo).*
>
> *Las víctimas de ciberdelincuencia no siempre encuentran la asistencia adecuada para reparar los daños sufridos y, a menudo, no denuncian los delitos. En particular, los menores y las personas de edad avanzada pueden carecer de las capacidades digitales necesarias o desconocer las vías de actuación que tienen a su alcance. Debe facilitarse aún más la denuncia de la ciberdelincuencia y debe proporcionarse a las víctimas la ayuda que necesitan»*[2].

La Relatora Especial, Sra. Dubravka Šimonović, en el *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos* de ONU Mujeres de 2018[3], aborda los nuevos desafíos que plantea esta violencia, incluyendo la prevención, la protección, el enjuiciamiento y la reparación de tales actos. Este informe señala que, si bien el uso de la tecnología de la información y las comunicaciones ha contribuido al empoderamiento de las mujeres y las niñas, así como a una mayor realización de sus derechos humanos, es necesario examinar este fenómeno y la aplicabilidad de las leyes nacionales a este respecto. Asimismo, menciona la necesidad de formular recomendaciones a los Estados y a los actores no estatales para combatirla, respetando, al mismo tiempo, la libertad de expresión y la prohibición de incitación a la violencia y al odio, de conformidad con el artículo 20 del Pacto Internacional de Derechos Civiles y Políticos.

En este contexto, en marzo de 2019, el Comité de Ministros del Consejo de Europa adoptó la Recomendación sobre la prevención y la lucha contra el sexismo, donde se señala que:

> «*Internet ha proporcionado un nuevo espacio para la expresión y transmisión del sexismo, especialmente el discurso de odio sexista, a un amplio público, a pesar de que el origen del sexismo no se encuentra en la tecnología, sino en las persistentes desigualdades de género*»[4].

---

[2] UE. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de la UE sobre los derechos de las víctimas (2020-2025)*, 2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020DC0258

[3] ONU. *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos,* 2018. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F38%2F47&Language=E&DeviceType=Desktop&LangRequested=False

[4] CONSEJO DE EUROPA. *Recomendación CM/Rec(2019) del Comité de Ministros a los Estados miembros para prevenir y combatir el sexismo*, 2019. Disponible en: https://rm.coe.int/def-26-09-19-recomendacion-consejo-de-europa-sexismo/1680981feb

Por otra parte, el Grupo de Expertos en la lucha contra la violencia contra las mujeres y la violencia doméstica (GREVIO), en su Recomendación General número 1 sobre la dimensión digital de la violencia contra las mujeres, adoptada el 20 de octubre de 2021[5], reconoce la violencia contra las mujeres en el ámbito digital como un problema global cada vez más prevalente y con graves consecuencias. Con esta Recomendación General, el GREVIO busca establecer conceptos clave relacionados con la violencia contra las mujeres y la violencia doméstica perpetrada en la esfera digital, y plantear sugerencias en relación con los cuatro pilares del Convenio de Estambul: prevención, protección, persecución y políticas coordinadas. En este sentido, se debe mencionar la expresión «dimensión digital de la violencia contra la mujer», acuñada por la Plataforma de Mecanismos de Expertos Independientes sobre la Discriminación y la Violencia contra la Mujer (Plataforma EDVAW) en su *Primer documento temático sobre la dimensión digital de la violencia contra las mujeres abordada por sus siete mecanismos* (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»[6].

Este término se emplea para enfatizar el hecho de que este comportamiento dañino se dirige desproporcionadamente hacia las mujeres y las niñas. La dimensión digital de la violencia contra las mujeres y niñas abarca una amplia gama de actos en el ciberespacio o a través de la tecnología, que forman parte del continuo de violencia que experimentan por razones relacionadas con su género y que constituyen manifestaciones tan dañinas o más que otras formas de violencia machista. En este sentido, cabe destacar la existencia de textos que aluden a la prevención y la lucha contra el sexismo y los discursos de odio sexista como, por ejemplo, la Recomendación no vinculante CM/Rec(2019) del Comité de Ministros a los Estados miembros para prevenir y combatir el sexismo[7], que incluye una sección dedicada al discurso de odio sexista en línea y la Recomendación General Política de la Comisión Europea contra el Racismo y la Intolerancia (ECRI) sobre la lucha contra el discurso de odio[8]. En este

---

[5] GREVIO. *Recomendación General nº1 sobre la dimensión digital de la violencia contra la mujer*, 2021. Disponible en: https://violenciagenero.org/web/wp-content/uploads/2022/01/rec_1_grevio.pdf

[6] CONSEJO DE EUROPA. *La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW*, 2022. Disponible en: https://www.ohchr.org/sites/default/files/documents/hrbodies/cedaw/statements/2022-12-02/EDVAW-Platform-thematic-paper-on-the-digital-dimension-of-VAW_Spanish.pdf

[7] CONSEJO DE EUROPA. *Recomendación CM/Rec(2019) del Comité de Ministros a los Estados miembros para prevenir y combatir el sexismo*, 2019. Disponible en: https://rm.coe.int/def-26-09-19-recomendacion-consejo-de-europa-sexismo/1680981feb

[8] CONSEJO DE EUROPA. *Recomendación General nº 15 relativa a la lucha contra el discurso de odio y memorándum explicativo*, 2015. Disponible en: https://rm.coe.int/09000016808b7904

sentido, se señala la Recomendación General número 35 del Comité CEDAW[9], que refleja la dimensión digital de la violencia contra la mujer y advierte que puede suponer un impacto significativo en su vida, limitando su libertad de expresión, su participación en la vida pública y su acceso a oportunidades en línea. Además, puede tener consecuencias graves para su salud física y mental.

Por último, es imprescindible mencionar la conocida como *«Ley Olimpia»*, que se trata de un conjunto de reformas legislativas en distintos estados de México, encaminadas a reconocer la violencia digital y penalizar aquellos delitos cometidos empleando medios digitales que atenten contra la intimidad sexual de las personas[10]. Además, ha tenido importantes repercusiones internacionales, influyendo en otros países como Argentina y Chile (en este país ha sido nombrada como «*Ley Belén*[11]»).

Este escenario manifiesta la necesidad de articular soluciones para las nuevas situaciones ilícitas derivadas del uso inadecuado de la tecnología, tanto para las personas menores de edad como para las mujeres, así como de determinar las posibles lagunas y vacíos legales que dificultan su protección efectiva. En definitiva, esta transformación digital implica nuevos retos que hay que afrontar en cuanto a crear un entorno en línea seguro, predecible y digno de confianza.

2. OBJETIVOS

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. Especialmente, examinar la legislación española.
- Diagnosticar la influencia del contenido para personas adultas[12] en personas menores de edad en relación con la normalización de conductas.

---

[9] ONU. Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW). *Recomendación general núm. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19*, 2017. Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2017/11405.pdf

[10] DÍAZ, P.; «Ni porno ni venganza: violencia digital, afirma la inspiradora de la Ley Olimpia en México», *Noticias ONU. Mirada global Historias humanas*, 8 de marzo de 2023. Disponible en: https://news.un.org/es/story/2023/03/1519217

[11] Proyecto de Ley Belén. Argentina, 2022. Disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2024/PDF2024/TP2024/1123-D-2024.pdf

[12] Por tal se entiende el contenido sexual explícito violento o inadecuado fuera de un contexto de educación sexual y contenido violento de cualquier naturaleza.

- Evaluar la repercusión de las nuevas tecnologías de la información y de la comunicación en la perpetuación y consolidación de los roles de género, así como 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.

3. METODOLOGÍA

Con el fin de dar respuesta a los objetivos planteados, se ha empleado una metodología cualitativa para comprender la conceptualización, la naturaleza y las características inherentes a la violencia digital contra las mujeres y personas menores de edad. Dentro de esta investigación cualitativa, se han utilizado dos herramientas: una, el análisis y estudio de investigaciones, normativas y diversas fuentes bibliográficas; y la otra, la realización un grupo focal de personas expertas. En cuanto a la primera herramienta, se ha estudiado de forma pormenorizada el marco normativo y la codificación de los delitos cometidos a través de las nuevas tecnologías. Además, se han observado las nuevas formas de control y de poder que se ejercen hacia las mujeres y las personas menores de edad a través de las redes sociales mediante el instrumento tecnológico.

En relación con el grupo focal, se ha celebrado un encuentro de profesionales para reflexionar y debatir sobre la violencia digital. Previamente, los y las distintas profesionales han dado respuesta a un formulario de preguntas cerradas con el fin de debatir las consideraciones proporcionadas desde los diversos ámbitos. Esto ha permitido, entre otras cosas, obtener una radiografía más completa del alcance de esta forma de violencia con el fin de detectar las posibles deficiencias y las buenas prácticas.

4. ESTRUCTURA DEL ESTUDIO

Este estudio se divide en tres grandes bloques, que convergen en la finalidad última de obtener un panorama general del ámbito normativo y detectar los déficits en las herramientas con las que se cuenta actualmente para la prevención, protección y tutela de las mujeres y las personas menores de edad a través de un enfoque multidisciplinar y coordinado entre los diferentes actores involucrados.

El primer bloque busca un acercamiento a la realidad de la violencia digital. Para ello, se revisa su conceptualización y se ofrece una radiografía de la evolución de las nuevas tecnologías de la información y de la comunicación en su utilización como otro medio más de control y de acoso sobre las mismas. Igualmente, se estudia la influencia de las TIC en la movilización del movimiento feminista.

En el segundo apartado, el foco de atención se pone sobre las personas menores de edad, ya que su relación con las nuevas tecnologías es directa y constante, lo que implica un mayor riesgo de sufrir determinados delitos, como el ciberacoso o el *grooming.* De la misma manera, se observa la importancia que tiene el papel de la educación y de la formación de las personas menores de edad en

un buen uso de Internet. Por otra parte, se pretende comprobar la facilidad de su acceso a contenidos para adultos.

Por último, la tercera sección está dedicada a la revisión del marco legislativo tanto internacional como europeo y nacional, en relación con la tipificación penal de los delitos del entorno digital y el valor de la prueba digital en el proceso judicial, así como la problemática de la transnacionalidad.

En la parte final del estudio, una vez realizado el análisis cualitativo y recogidas unas conclusiones, se presentan una serie de propuestas y recomendaciones para tener un entorno digital seguro, saludable y libre de violencia a la ciudadanía, especialmente a las mujeres y a las personas menores de edad.

CAPÍTULO I.
APROXIMACIÓN A LA REALIDAD DE LA VIOLENCIA DIGITAL

1. CONCEPTO

En la actualidad, no existe una definición universal única y uniforme de «violencia digital». A diferencia de otras clases de violencia, que sí son contempladas normativamente, las alusiones a los ataques que sufren las mujeres y las niñas en el entorno virtual precisan de una delimitación y conceptuación que todavía no se ha formulado. Aunque sí existen referencias a la misma en diferentes documentos y textos normativos, que pasamos a exponer.

El Consejo de Europa definió la ciberviolencia 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*»[13].

Por su parte, la Relatora Especial sobre la Violencia contra las Mujeres 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*»[14].

El Comité Consultivo de Igualdad de Oportunidades para Mujeres y Hombres de la Comisión Europea recomienda, en notificación de 2020 a la Unión Europea y a sus Estados miembros, el reconocimiento de la ciberviolencia como una forma de violencia contra las mujeres. Este Comité, basándose en los conceptos proporcionados por el Consejo de Europa y Naciones Unidas, invita a utilizar la siguiente definición:

> «*La ciberviolencia contra la mujer es un acto de violencia de género perpetrado directa o indirectamente a través de las tecnologías de la información y la comunicación que tiene como resultado, o es probable que tenga como resultado, daños físicos, sexuales, psicológicos o daño económico o sufrimiento a las mujeres y las niñas, incluidas las amenazas de tales actos, ya sea que ocurran en la vida pública o privada, o los obstáculos al ejercicio de sus derechos y libertades fundamentales. La violencia cibernética contra las mujeres no se limita a, sino que incluye, violaciones de la privacidad, acecho, acoso, violencia basada en el género, incitación al odio, intercambio de contenido personal sin consentimiento, abuso sexual basado en imágenes,*

---

13 CONSEJO DE EUROPA. *Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018*. Disponible en: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914

14 ONU. *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*, 2018. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F38%2F47&Language=E&DeviceType=Desktop&LangRequested=False

piratería informática, robo de identidad y violencia directa. La ciberviolencia es parte del continuo de la violencia contra las mujeres: no existe en el vacío; más bien, se deriva y sostiene múltiples formas de violencia fuera de línea»[15].

Junto a ello, el Convenio de Estambul[16], norma de referencia en materia de violencia de género desde su aprobación, no contiene una alusión explícita a la dimensión digital de la violencia contra las mujeres, lo que resulta razonable dado el momento de elaboración del mismo. Sin embargo, incluye todas las formas de violencia contra las mujeres cuando determina su ámbito de aplicación (artículo 2). Por ende, la violencia digital quedaría englobada dentro de este precepto. Además, en concreto, sus artículos 33, 34 y 40 son aplicables al contexto digital, pues contemplan acciones como el acoso o el acoso sexual, que se reconocen como clases de violencia psicológica y que se utilizan como elementos de ejemplificación para delimitar los contornos de la ciberviolencia. Asimismo, el Convenio anima tanto al sector privado como al sector de las TIC y de los medios de comunicación a participar en la elaboración y aplicación de políticas integradoras y a establecer directrices para prevenir la violencia contra la mujer, reforzando el respeto de su dignidad. También, incita a promover las capacidades de las y los menores, progenitores y personas educadoras para hacer frente a un entorno tecnológico seguro (artículo 17).

Deteniéndonos en el artículo 40 del Convenio, la previsión referente al acoso sexual es aplicable tanto al acoso sexual analógico como en línea y/o facilitado por la tecnología, puesto que con arreglo a su definición constituye tal acoso: «*toda forma de comportamiento no deseado, verbal, no verbal o físico, de carácter sexual, que tenga por objeto o resultado violar la dignidad de una persona, en particular cuando dicho comportamiento cree un ambiente intimidatorio, hostil, degradante, humillante u ofensivo*». Igualmente, la disposición del Convenio en materia de acoso (artículo 34) también sería aplicable al ejercido en línea, ya que «*el hecho, cuando se cometa intencionadamente, de adoptar en varias ocasiones un comportamiento amenazador contra otra persona, que lleve a ésta a temer por su seguridad*».

Esta extensión del ámbito de aplicación a la esfera digital ha sido confirmada por el *Informe Explicativo del Convenio del Consejo de Europa sobre la prevención y lucha de violencia de género y doméstica*[17], que explícitamente clasifica como contacto no deseado «*la búsqueda de cualquier contacto activo con la víctima a través de cualquier medio de comunicación disponible, incluidas las herramientas modernas de comunicación y las TIC*». En vista de las graves consecuencias psicológicas que la violencia en línea puede tener sobre las víctimas, el requisito del Convenio de Estambul de tipificar como delito la violencia psicológica (artículo 33) reviste un sentido importante[18].

---

15 UE. Comité Consultivo de Igualdad de Oportunidades entre hombres y mujeres de la Unión Europea. *«New notification: cyberviolence against women has been flagged» Opinion on combatting online violence against women*, 2020. Disponible en: https://commission.europa.eu/document/download/eae53eb9-ca88-4fc0-8a6e-51e771c96f68_en?filename=opinion_online_violence_against_women_2020_en.pdf

16 CONSEJO DE EUROPA. *Convenio del Consejo de Europa sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica*, 2011. Disponible en https://rm.coe.int/1680462543

17 CONSEJO DE EUROPA. *Informe Explicativo del Convenio del Consejo de Europa sobre la prevención y lucha de violencia de género y doméstica*, 2011. Disponible en: https://rm.coe.int/1680a48903

18 CONSEJO DE EUROPA. *Proteger a las mujeres y niñas de la violencia en la era digital. La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra*

Si bien el Convenio de Estambul ofrece un marco legal que debe ser completado para delimitar la dimensión digital de la violencia con otros tratados relevantes, como el Convenio sobre Ciberdelincuencia del Consejo de Europa (conocido como Convenio de Budapest) y sus protocolos. En esta línea, el Consejo de Europa recomienda tanto a las Partes del Convenio de Estambul abordar la dimensión digital como a las del Convenio de Budapest, y en caso necesario, a adoptar una nueva legislación que se adecúe a las nuevas formas de violencia digital.

Como se ha mencionado, la violencia digital hacia las mujeres y las personas menores de edad es una extensión de las otras formas de violencia ya existentes (física, psicológica, económica, etc.). La mayoría de estos modos de agresiones virtuales constituyen crímenes, contemplados ya como delitos, que amplifican el daño cuando se cometen a través del instrumento digital, como es el caso de la violencia doméstica. GING y SIAPERA aseveran que:

> «*El troleo, el abuso verbal, la sextorsión, el intercambio no consentido de imágenes íntimas, la manipulación de fotos, el ciberacoso, el doxeo, la piratería informática, las infracciones de la propiedad intelectual y los ataques DDoS*[19] *pueden ocurrir exclusivamente en línea, pero también pueden tener lugar en relación con hechos fuera de línea, y casi siempre tienen repercusiones que se experimentan tanto en línea como fuera de línea*»[20].

En este sentido, el Consejo de Europa, en su informe *Proteger a las mujeres y niñas de la violencia en la era digital*[21], señala que las formas de violencia contra las mujeres facilitadas por la tecnología incluyen las siguientes manifestaciones, pero no se limitan a ellas:

1. El acoso sexual en línea, que incluye el exhibicionismo cibernético (*cyberflashing*) o envío de imágenes sexuales no solicitadas; los comentarios sexualizados; la difamación sexualizada; la suplantación de identidad con fines sexuales; el *doxeo*[22] (*doxing*); el *troleo*[23] (*trolling*) sexualizado y basado en el género; el *flameo*[24] (*flaming*); los ataques de pandillas (*mob attacks*); el acoso

---

las mujeres en línea y facilitada por la tecnología, 2021. Disponible en: https://rm.coe.int/study-istanbul-convention-and-budapest-convention-/1680a62700

[19] DDoS es un ataque distribuido de denegación de servicio, un tipo de ciberataque, en el que un atacante sobrecarga un sitio web, un servidor o un recurso de red con tráfico malicioso.

[20] GING, D., SIAPERA, E.; «Special issue on online misogyny», Feminist Media Studies, *Routledge Taylor & Francis Group,* 2018, v. 18, n.º 4, pp. 515-524. Disponible en: https://doi.org/10.1080/14680777.2018.1447345

[21] CONSEJO DE EUROPA. *Proteger a las mujeres y niñas de la violencia en la era digital. La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología*, 2021. Disponible en: file:///D:/USUARIOS/Usuario04/Descargas/047722ESP_violencia%20en%20era%20digital%20(1).pdf

[22] *Doxing o doxeo,* consiste en reunir y difundir datos personales de una persona o un grupo sin su autorización, con la intención de perjudicar su reputación pública y profesional.

[23] *Trolling o troleo*, Son comportamientos en línea habitualmente anónimos, que tienen como objetivo incomodar, agredir verbalmente, provocar o causar daño mediante mensajes den redes sociales, blogs o foros, con intención de perjudicar la reputación de alguien o propagar información engañosa.

[24] *Flaming o flameo*, se refiere a agredir verbalmente a alguien en internet. Implica el uso de insultos, la expresión de intolerancia y cualquier forma de hostilidad verbal dirigida a una persona en particular

sexual basado en imágenes, como las fotos rastreras (*creepshots* –fotos sexualmente sugerentes o íntimas tomadas sin consentimiento y difundidas en línea–); las fotos debajo de la falda (*upskirting* –fotos sexuales o íntimas tomadas debajo de la falda o el vestido sin consentimiento y difundidas en línea–); el abuso sexual basado en imágenes (difusión no consentida de imágenes, vídeos o imágenes íntimas); la «pornografía de venganza»; las «ultrafalsas»[25] (*deepfakes*); las agresiones sexuales y las violaciones grabadas, incluidas las «videoagresiones» (*happy slapping*) transmitidas en vivo o distribuidas en sitios pornográficos; las amenazas y la coerción como el sexteo forzado (*forced sexting*), la *sextorsión*; las amenazas de violación, y la incitación a cometer una violación.

2. Formas de acoso, vigilancia o espionaje en línea empleando redes sociales o mensajería; robo de contraseñas; descifrado o piratería de dispositivos; instalación de *software* espía; suplantación de identidad con fines de acoso; geolocalización o localización mediante GPS; intimidación; amenazas y el control mediante cerraduras inteligentes o electrodomésticos inteligentes.

3. Formas de violencia psicológica, como el discurso de odio sexista en línea; la incitación a las autolesiones o al suicidio; las agresiones verbales; los insultos; las amenazas de muerte; las presiones; el chantaje, y el revelar el nombre anterior (*deadnaming*), es decir, emplear en contra de su voluntad el nombre con que fue inscrita en su nacimiento una persona transexual con el fin de perjudicarla.

A partir de esta clasificación y, ante una falta de categorización unánime de las tipologías de ciberviolencia, en España el Observatorio Nacional de Tecnología y Sociedad (organismo dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial) realiza la siguiente:

1. Ciberacoso. Amenazas de violencia (incluida la sexual), coacción, insultos o amenazas, difusión no consentida de imágenes sexualmente explícitas.

2. Amenazas directas o violencia física relacionada con las tecnologías digitales.

3. Crímenes de odio relacionados con las tecnologías digitales. En el caso que nos ocupa, por razón de sexo.

4. Violaciones de privacidad relacionadas con la digitalización e Internet. *Doxing* (revelación de información personal confidencial), robos o suplantaciones de identidad, o tomar, compartir y manipular datos o imágenes (incluidos datos íntimos).

5. Explotación sexual *online*.

Además, el Instituto Europeo de la Igualdad de Género (*European Institute for Gender Equality-EIGE*), en su estudio *La ciberviolencia contra las mujeres y niñas*[26], incluye dentro del concepto de ciberviolencia el ciberhostigamiento, el ciberacoso y la pornografía no consentida.

---

[25] *Deepfake*, es un contenido audiovisual, ya sea un video, una imagen o un audio, manipulados con tecnología de inteligencia artificial de modo que parezcan auténticos, genuinos y reales.

[26] EIGE. *La ciberviolencia contra las mujeres y niñas*, 2017. Disponible en: https://eige.europa.eu/sites/default/files/documents/ti_pubpdf_mh0417543esn_pdfweb_20171026164000.pdf

En cuanto a España, como bien puntualiza LLORIA GARCÍA, tampoco existe una definición normativa común de violencia digital. Las primeras referencias a la misma, de una manera abierta y ceñida al ámbito de la violencia sobre las mujeres y sobre las personas menores de edad, 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. En estas normas, se hace una enumeración de actos que pueden conformar el concepto, sin llegar a definirlo (en los artículos 1.2 y 3 respectivamente). Las menciones que se contienen en estos preceptos pueden servir como punto de partida para la conformación de un concepto más concreto, que es una tarea que queda pendiente todavía[27].

Por último, la reciente 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[28], 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, lo que resulta sorprendente, pues el artículo 4 del texto de la Propuesta de Directiva sí lo establecía:

> «*todo acto de violencia regulado por la presente Directiva cometido, asistido o agravado en parte o en su totalidad mediante el uso de las tecnologías de la información y de las comunicaciones*»[29].

De esta forma, se ha perdido la oportunidad de proporcionar una definición que fuera única para el territorio de la Unión, lo que facilitaría mucho el desarrollo de las normativas comunes en la materia.

Por lo tanto, y en atención a lo expuesto, se puede afirmar que la ciberviolencia se contempla como una clase de violencia psicológica, que utiliza el medio tecnológico para manifestarse o producirse, que afecta a las mujeres y a las niñas de forma desproporcionada, y en los listados que se exponen no se toman en consideración ni la totalidad de actuaciones que pueden entrar dentro de la misma, ni las consecuencias que el uso de dicho instrumento o el lugar donde se cometa –el ciberespacio– pueda tener en relación con la lesión que dicha violencia genera.

2. DATOS ESTADÍSTICOS

A pesar de la falta de estadísticas más específicas e interrelacionadas con los diferentes delitos tipificados en el entorno nacional y europeo, se puede afirmar, atendiendo a los datos disponibles,

---

[27] LLORIA GARCÍA, P.; «La LO 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia y la transformación del Código Penal. Algunas consideraciones», *Igualdad.ES*, n.º 6, enero-junio 2022, pp. 271-298. Disponible en: https://www.cepc.gob.es/sites/default/files/2022-07/39798igdes609lloria-gacia.pdf

[28] UE. Directiva (UE) 2024/1385 del PARLAMENTO EUROPEO y del CONSEJO, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, 2024. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80770

[29] UE. Propuesta de DIRECTIVA DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la lucha contra la violencia contra las mujeres y la violencia doméstica (COM/2022/105 final), 2022. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0105

que la violencia digital afecta mayoritariamente a mujeres y niñas. Si bien en los últimos años se han realizado un mayor número de estudios sobre la violencia digital, esta escasez de información dificulta la determinación de la verdadera y real dimensión del problema.

Aun así, se puede asegurar que la violencia virtual o ciberviolencia es una extensión de la violencia que se ejerce contra las mujeres y las niñas fuera del ámbito digital, lo cual demuestra que las desigualdades estructurales de género también se reproducen en el ciberespacio[30].

En términos digitales, la difusión de vídeos e imágenes sexuales sin consentimiento es una realidad que afecta en un porcentaje mayor a las mujeres. Al respecto, la ONU[31] indica, entre los datos más relevantes, los siguientes: más del 73 % de las mujeres de ámbito mundial han sido expuestas o han experimentado algún tipo de violencia en Internet, las jóvenes de 18 a 24 años se enfrentan a un alto riesgo de sufrir persecución, acoso sexual y amenazas físicas. En los 28 países de la Unión Europea, nueve millones de mujeres han experimentado violencia en línea desde los 15 años y una de cada cinco mujeres usuarias de Internet reside en países donde es poco probable que se castigue el acoso y abuso en línea hacia las mujeres. Igualmente, el 28 % de las que han sido víctimas de violencia en línea han decidido disminuir su actividad en Internet de forma intencionada y el 90 % de las víctimas de distribución de imágenes íntimas de contenido sexual sin consentimiento son mujeres[32].

Por su parte, la Agencia Europea para la Protección de los Derechos Fundamentales (FRA, *European Union Agency for Fundamental Rights*) es una de las primeras en recabar datos sobre el acoso cibernético hacia las mujeres y el acoso sexual cometido a través de las nuevas tecnologías. Los ítems incluidos en la encuesta recogida en el estudio *Violencia de Género contra las mujeres: una encuesta a escala de la UE*[33] (2014) en relación con el acoso sexual y la intensidad con que se han producido son los siguientes:

- Imágenes, fotografías o regalos que alguien le envió o mostró, de contenido sexualmente explícito, que le ofendieron.

---

30 Distintas autoras han trabajado sobre este aspecto. Por ejemplo: ARÁNGUEZ SÁNCHEZ, T. y OLARIU O. *Feminismo digital. Violencia contra las mujeres y brecha sexista en internet*, 2021. Disponible en: https://repositorio.comillas.edu/rest/bitstreams/484918/retrieve. VILLEGA-SIMÓN, I. y NAVARRO, C. *Influencers digitales y el feminismo: del activismo al self-branding*, 2021. QUERALT JIMÉNEZ, A.; «Desinformación por razón de sexo y redes sociales», *International Journal of Constitutional Law*, v. 21, n.º 5, 2023, pp. 1589–1619. Disponible en: https://www.politico.eu/wp-content/uploads/2024/03/06/moad0941.pdf

31 ONU. *Combatir la violencia en línea contra las mujeres y las niñas: Una llamada de atención al mundo,* 2015. Disponible en: https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf

32 ONU. *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*, 2018. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F38%2F47&Language=E&DeviceType=Desktop&LangRequested=False

33 UE. Agencia Europea de los Derechos Fundamentales (FRA). *Violencia de Género contra las mujeres: una encuesta a escala de la UE, 2014.* Disponible en: https://fra.europa.eu/sites/default/files/fra-2014-vaw-survey-at-a-glance-oct14_es.pdf

- Material pornográfico que alguien le obligó a ver en contra de su voluntad.
- Mensajes de correo electrónico o SMS (servicios de mensajes cortos) sexualmente explícitos ofensivos.
- Insinuaciones inapropiadas, humillantes y vejatorias en redes sociales, como Facebook, o foros de Internet.

Los resultados de la encuesta revelaron que una de cada diez mujeres (un 11 %) han recibido insinuaciones inadecuadas en redes sociales o mensajes de correo electrónico o de texto con contenido sexual explícito. Esta forma de acoso sexual afecta mayoritariamente a mujeres jóvenes. Este muestreo indica que 1,5 millones de mujeres en la Unión Europea de entre 18 y 29 años son víctimas de acoso cibernético en los doce meses previos a la entrevista. El peligro de que las mujeres de entre 18 y 29 años sean destinatarias de este tipo de acoso es el doble que el de las mujeres de 40 a 49 años y más del triple que las de 50 a 59 años[34].

Merece la pena destacar que, de todas las mujeres que han sufrido acoso por medio de correo electrónico, mensajes de texto o Internet, un 21 % manifiesta que dicho acoso se prolonga en el tiempo durante más de dos años. Y una de cada cinco mujeres que reciben este tipo de acoso tuvieron que cambiar su dirección de correo electrónico o número de teléfono, siendo un indicador que nos sirve para determinar la existencia de un verdadero acoso, desde el punto de vista jurídico, que exige reiteración y cambio en los hábitos de vida.

El *Informe Ciberviolencia contra las mujeres y las niñas. Una llamada de alerta al mundo*[35], publicado por la Comisión de Banda Ancha de la ONU en septiembre de 2015, señala que casi las tres cuartas partes de las mujeres han estado expuestas a alguna forma de violencia en línea. Según el informe, un 73 % de mujeres ha experimentado algún tipo de agresión en Internet y un 18 % ha sufrido violencia en línea a edades tempranas, como son los 15 años[36].

Igualmente, cabe mencionar la investigación llevada a cabo por Amnistía Internacional sobre el impacto que tienen en las mujeres los abusos y el acoso en las redes sociales. Esta encuesta de 2017 realiza un sondeo sobre las experiencias de mujeres de entre 18 y 55 años en Dinamarca, España, EE. UU., Italia, Nueva Zelanda, Polonia, Reino Unido y Suecia de las consecuencias alarmantes que suponen los abusos hacia las mujeres en Internet: un 61 % sufre baja autoestima o pérdida de confianza en sí mismas; un 55 % padece estrés, ansiedad o ataques de pánico; un 63 % revela que tienen problemas para dormir, y un 56 %, falta de concentración. La investigación evidencia que un 41 % de las mujeres víctimas de ataques en Internet afirman que, al menos una vez, sintieron amenazada su integridad física. Y un 26 % de las mujeres que recibieron acoso manifiestan que, además, se desvelaron públicamente datos personales de ellas y, de esta forma, podían ser identificadas (este acto es el conocido como *doxing, doxxing* y *doxeo*).

---

34 *Ibidem.*

35 ONU. *Combatir la violencia en línea contra las mujeres y las niñas: Una llamada de atención al mundo,* 2015. Disponible en: https://networkedintelligence.com/wp-content/uploads/2019/02/Cyber_violence_Gender-report.pdf

36 *Ibidem.*

De acuerdo con Amnistía Internacional, el acoso cibernético ha llevado al 76 % de las mujeres a cambiar la forma en que utilizan las redes sociales, y al 32 % a dejar de expresar sus opiniones sobre temas específicos[37]. Este tipo de violencia en Internet basada en el género puede extenderse de una manera rápida y fácil. Y también, conducir a una violencia fuera de línea.

Es especialmente notable, la Encuesta Europea de Violencia de Género (EEVG)[38], desarrollada por la Delegación de Gobierno contra la Violencia de Género, ya que, por primera vez, se lleva a cabo un estudio sobre la violencia contra las mujeres en el contexto del Sistema Estadístico Europeo (SEE)[39], el cual es coordinado por Eurostat (Comisión Europea). Este sistema garantiza que la información recopilada por los distintos Estados miembros de la Unión Europea sea confiable, al seguir parámetros y conceptos comunes y asegurar un tratamiento adecuado de los datos estadísticos para facilitar su comparación entre los países. La encuesta ofrece información sobre la prevalencia de la violencia hacia las mujeres, abarcando sus distintas modalidades, así como detalles sobre la frecuencia y la gravedad de estas manifestaciones. En total, han participado 27 países de la Unión Europea y otros, incluidos Islandia, Montenegro, Serbia, Norte de Macedonia y Kosovo. La investigación se centra en mujeres europeas de entre 18 y 74 años, aunque en nuestro país se ha incluido a mujeres desde los 16 años para recopilar información sobre la población de mujeres más jóvenes.

La Encuesta mencionada también aborda la creciente preocupación por los actos violentos que se cometen en el entorno digital; entre estos, destacan el stalking y el acoso sexual en el trabajo. Este trabajo busca ofrecer una visión integral de cómo la violencia se manifiesta en diferentes formas, incluyendo aquellas que ocurren en línea, para así contribuir a la creación de estrategias más efectivas de prevención y apoyo.

En lo que respecta al acoso reiterado (stalking), se observa que el 19,5 % de las mujeres que residen en España, con edades comprendidas entre 16 y 74 años, ha experimentado esta forma de acoso en algún momento de su vida. Esto representa aproximadamente 3.478.008 mujeres. En cuanto a los tipos de violencia que han sufrido, el 11,0 % ha recibido mensajes, correos electrónicos, cartas o regalos no deseados de manera repetida. Además, el 8,6 % ha sido blanco de llamadas telefónicas obscenas, amenazantes, molestas o silenciosas, mientras que el 0,9 % ha visto divulgadas imágenes, vídeos o información altamente personal sobre ellas.

Es importante señalar que experimentan acoso de manera reiterada un 30,6 % de las mujeres entre los 16 y 17 años, y un 33% entre 18 y 29. Además, se observa que un 85,8% de los agresores son hombres.

---

[37] ESPAÑA. Delegación del Gobierno contra la Violencia de género. *El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento*, 2017. Disponible en: https://violenciagenero.igualdad.gob.es/wp-content/uploads/Libro_18_Ciberacoso-2.pdf

[38] ESPAÑA. Delegación del Gobierno contra la Violencia de género. *Encuesta Europea de Violencia de Género 2022.*Disponible en: https://violenciagenero.igualdad.gob.es/wp-content/uploads/EEVG.pdf

[39] Sistema Estadístico Europeo (SEE) está formado por: Eurostat (la oficina estadística de la UE), las oficinas de estadística de todos los estados miembros (los diferentes INE) y otros organismos que elaboran estadísticas europeas.

En cuanto al acoso sexual en el ámbito laboral hacia las mujeres, comportamientos no solicitados de carácter sexual en el entorno profesional, es importante destacar que el 3,0 % de las mujeres han tenido que afrontar la visualización de imágenes o vídeos sexualmente explícitos, lo que les ha causado ofensa, humillación o intimidación. Además, un 5,4 % ha recibido insinuaciones indebidas a través de redes sociales, y un 3,3 % ha sido objeto de correos electrónicos o mensajes de texto inapropiados y sexualmente explícitos.

En el ámbito del acoso sexual laboral, el 88,5 % de los agresores son hombres, similar a lo que se observa en el stalking, donde también predominan los hombres como agresores.

Respecto a la búsqueda de apoyo, son muy pocas las víctimas de acoso sexual en el ámbito laboral que denuncian el incidente a la policía en un 3,2 %. En cambio, este porcentaje aumenta en el caso del acoso persistente (stalking) que alcanza el 13,9 %.

Según la Estrategia de Igualdad de género 2020-2025, que tiene como objetivo principal abordar la igualdad de género, uno de los valores fundamentales de la Unión Europea a través de acciones políticas concretas, con arreglo a los datos del Eurobarómetro de 2022 en relación con la ciberviolencia de género, se encontró que el 16 % de las mujeres entrevistadas en la UE conocían a otra mujer que había experimentado este tipo de violencia digital.

Por otro lado, en relación con las cifras de nuestro país, la *Macroencuesta de Violencia contra la Mujer 2019* de la Delegación del Gobierno contra la Violencia de Género[40] apunta a que un 18,4 % de las mujeres que afirman haber sufrido algún tipo de acoso sexual, han recibido insinuaciones inapropiadas, humillantes, intimidatorias u ofensivas en las redes sociales de Internet como *Facebook, Instagram o Twitter*. De la misma forma, un 15,9 % han recibido correos electrónicos, mensajes de *WhatsApp,* o mensajes de texto sexualmente explícitos inapropiados, que las han hecho sentirse ofendidas, humilladas o intimidadas.

En este sentido, el informe *(IN)SEGURAS ONLINE: Resultados de España* de la ONG Plan International[41], publicado en 2020, destaca que en nuestro país:

- El 59 % de las niñas y jóvenes han sufrido alguna forma de acoso *online* en distintas redes sociales.
- De las jóvenes y niñas que no se han enfrentado a ningún tipo de acoso *online* por razón de género, el 34 % conocen a otras chicas o jóvenes que sí lo han experimentado.
- La mayoría de las chicas empiezan a padecer acoso *online* entre los 12 y los 16 años.
- El 77 % manifiestan que frecuentemente, o muy frecuentemente, han estado expuestas a un lenguaje ofensivo y abusivo; un 64 % afirma que han sido avergonzadas o humilladas públicamente por su físico y, de este porcentaje, el 41 % afirman recibir estos ataques con frecuencia o mucha frecuencia. Por último, el 58 % han sido acosadas sexualmente.

---

40 ESPAÑA. Delegación del Gobierno contra la Violencia de Género. *Macroencuesta de Violencia contra la Mujer,* 2019. Disponible en: https://violenciagenero.igualdad.gob.es/violenciaEnCifras/macroencuesta2015/Macroencuesta2019/home.htm

41 PLAN INTERNATIONAL. *Inseguras online, 2020*. Disponible en: https://plan-international.es/files_informes/Datos_Epana.pdf

- El 75 % de las niñas y jóvenes indican que han sido acosadas por gente a la que conocen.
- El 72 % han experimentado consecuencias negativas a raíz del acoso *online* sufrido: baja autoestima, pérdida de confianza, inseguridad por el físico, estrés mental o emocional.

Y *el Informe sobre delitos contra la libertad sexual de 2023* del Ministerio del Interior destaca que un 66 % de las victimizaciones registradas de ciberdelincuencia sexual son mujeres, mientras que un 96 % de los ciberdelincuentes sexuales investigados o detenidos son hombres y el 86,3% son nacionales[42]. Según esta estadística, el 84,8 % de las víctimas son menores de 18 años (de dicho porcentaje, el 47,6 % son menores de 13 años); respecto a la tipología penal, destacan los siguientes delitos contra la libertad sexual: pornografía infantil, contacto con menores de 16 años a través de la tecnología con fines sexuales y corrupción de menores/personas con discapacidad y acoso sexual. En cuanto a la distribución porcentual de investigados/detenidos, este mismo informe señala que recaen sobre hombres los siguientes datos: por pornografía de menores, en un 96 %; por acoso sexual, promoción a la prostitución a través de nuevas tecnologías, exhibicionismo, provocación sexual y delitos relativos a la prostitución, en un 100 %[43].

Por otra parte, en este epígrafe también es interesante conocer la percepción de la población sobre los delitos sexuales *online*. En este sentido, es reveladora la encuesta *Flash* Eurobarómetro sobre «*Protección de los niños contra el abuso sexual en línea*»[44]. Muestra que el 73 % de los y las europeas consideran que el abuso sexual infantil en línea es un problema generalizado o muy extendido, y el 92 % están de acuerdo en que los niños y las niñas corren cada vez más riesgos en el entorno digital. El 82 % de las personas encuestadas están de acuerdo en que herramientas como el control parental no son suficientes para mantener a los niños y a las niñas seguros en línea.

En suma, todos los datos especificados en este apartado muestran que esta violencia digital la sufren principalmente mujeres y menores. La violencia de género ha traspasado al mundo digital. Y las cifras demuestran la necesidad de educar en la concienciación sobre el uso responsable de las tecnologías, advertir de los riesgos, cómo reconocerlos y prevenirlos y el fomento de valores de igualdad y respeto.

3. EVOLUCIÓN DE LAS NUEVAS TECNOLOGÍAS

Desde la aparición de la Red de Servicios Integrados (RDSI)[45] en 1989, hasta la introducción de la fibra óptica, ha habido un crecimiento progresivo y exponencial de los canales de comunicación y las nuevas tecnologías. En los años 90, el uso de teléfonos móviles se disparó en todo el mundo. Los

---

42 ESPAÑA. Ministerio del Interior. *Informe sobre delitos contra la libertad sexual, 2023*. Disponible en: https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/INFORME-DELITOS-CONTRA-LA-LIBERTAD-SEXUAL-2023.pdf

43 *Ibidem.*

44 COMISIÓN EUROPEA. *Flash Eurobarometer Protection of children against online sexual abuse*, 2023. Disponible en: https://europa.eu/eurobarometer/surveys/detail/2656

45 RDSI. Red de servicios integrados. Es una tecnología de telecomunicaciones que permite la transmisión de voz, datos y vídeo de forma digital a través de una red de telecomunicaciones. Esta tecnología ofrece una mayor calidad de transmisión y una mayor eficiencia en la gestión de los recursos de red.

servicios financieros comenzaron a ofrecerse por Internet y los medios de comunicación oral y escrita comenzaron su proceso de digitalización.

A partir de 2004, con la aparición de *Facebook* y *YouTube*, las redes sociales comenzaron su ascenso. Al mismo tiempo, se introdujo el acceso a Internet desde dispositivos móviles, lo que aumentó las posibilidades de conexión en términos de espacio y tiempo. Hoy en día, los teléfonos móviles se utilizan para tomar fotos y vídeos, navegar por la *web*, realizar tareas diarias y enviar mensajes instantáneos a través de aplicaciones como *WhatsApp*, que revolucionó el tradicional SMS en 2014.

Un dato significativo de este rápido aumento en el uso de Internet es el porcentaje de acceso a la red desde los hogares. En 2004, este porcentaje era de aproximadamente el 33,6 %, mientras que en 2023 alcanzó el 96,4 %, lo que supone un aumento de 62,80 puntos porcentuales. Además, el 82,6 % de los hogares cuentan con algún tipo de ordenador y el 99,5 % disponen de un teléfono móvil[46]. También las empresas han adaptado sus estrategias de publicidad y prestación de servicios a las nuevas realidades tecnológicas. El 78,5 % de las compañías tienen su propia página *web*. El teletrabajo se desarrolla en un 34,2% de las empresas con diez o más empleados/as, aumentando este porcentaje al 78,0 % en empresas de 250 empleados/as o más[47].

Es evidente que el mundo digital se ha integrado en nuestras vidas, sin importar nuestra edad o clase social. Utilizamos dispositivos conectados para controlar las luces de nuestra casa, contamos con aplicaciones y altavoces con asistentes virtuales, accedemos a noticias diarias, servicios bancarios y compartimos fotos y vídeos en Internet. Realizamos compras en línea, nuestros automóviles están equipados con conexión inalámbrica y expresamos nuestras opiniones en diversos foros *online*; utilizamos relojes digitales inteligentes, auriculares y bandas de ejercicio que nos brindan información sobre el número de pasos, distancias recorridas y horas de sueño. En resumen, el uso de Internet y dispositivos electrónicos se ha vuelto común en nuestra vida cotidiana.

En consecuencia, toda esta información que proporcionamos al realizar nuestras actividades en línea, como pueden ser las búsquedas efectuadas, compras, publicaciones en redes sociales, interacciones en sitios web, comentarios en blogs y foros y otros comportamientos, ya sea consciente o inconscientemente, se conoce como huella digital. Se trata del conjunto de datos rastreables de nuestra vida personal que dejamos en Internet. A medida que aumenta nuestra actividad en línea, la huella digital se vuelve más extensa y detallada. En la actualidad, la mayoría nos exponemos constantemente a través de publicaciones sobre nuestros gustos, viajes y otras actividades, muchas de ellas en tiempo real.

La información recopilada a través de nuestra identidad digital puede ser utilizada por múltiples personas y con distintos fines: marketing, anunciantes, realizar investigaciones de mercado o tomar decisiones personalizadas para ofertar servicios e información acorde a nuestras preferencias, gustos e ideología.

---

[46] INE. Datos estadísticos, 2020. Disponible en: https://www.ine.es/dyngs/INEbase/es/operacion.htm?c=Estadistica_C&cid=1254736176741&menu=ultiDatos&idp=1254735576692

[47] PEREZ MARTÍNEZ, J., FRÍAS BARROSO, Z., y UREÑA LÓPEZ, A.; «50 años de la red de redes. La evolución de Internet en España: del Tesys a la economía digital», 2018. Disponible en: https://www.ontsi.es/sites/ontsi/files/2022-01/50%20A%C3%B1os%20de%20la%20Red%20de%20Redes.pdf

Esta huella provoca que nuestra perspectiva o idea de las cosas quede limitada o influenciada por nuestras búsquedas y hacerlas depender de ellas. Además, puede ser empleada con propósitos maliciosos: suplantación de identidad, creación de perfiles falsos, fraudes o comisión de delitos en tu nombre.

Es crucial la gestión correcta de las redes sociales para proteger nuestra privacidad digital, así como tener en cuenta la impresión que generamos en el entorno virtual y comprender qué información se encuentra sobre nosotros en internet. La implementación de prácticas responsables en el uso de estas plataformas nos resguarda de posibles amenazas y vulneraciones a nuestra intimidad, a la vez que nos ofrece beneficios significativos para conservar el control sobre nuestros datos personales. Por tanto, ser conscientes de la existencia de nuestra huella digital y adoptar medidas para preservar nuestra privacidad y seguridad en línea. Esto implica ser selectivos con la información que compartimos, utilizar contraseñas seguras, mantener nuestros dispositivos actualizados y estar atentos a posibles riesgos y amenazas en el entorno digital. En relación con esta idea de autoprotección, es importante evitar que se transmute en una visión de autopuesta en peligro, lo cual podría llevar a focalizar la culpa en la víctima, algo que no resulta deseable, ni por la revictimización que implica, ni por la posible aplicación de una tesis de compensación de culpas.

4. LAS NUEVAS TECNOLOGÍAS Y EL MOVIMIENTO FEMINISTA

El uso de las tecnologías de la información y comunicación (TIC) ha permitido el empoderamiento de las mujeres y sus colectivos. Se ha convertido en un importante medio para contribuir a la organización de la acción colectiva feminista, visibilizar discursos de concienciación y reivindicación social a gran escala, así como aumentar el poder de convocatoria, superando las limitaciones espaciales que existen en el ámbito analógico.

Desde la perspectiva internacional, movimientos sociales como el «*Me too*» donde mujeres de diversos ámbitos y puntos geográficos denunciaron situaciones de violencia sexual, han generado un debate sobre el acoso y abuso sexual en la industria del cine, la música, la ciencia y la política en el entorno internacional. A través de un *hashtag*, se logró introducir en la agenda política de muchos países un tema tan relevante como la regulación y protección de las mujeres frente a este tipo de ataques[48]. Como señala GARCÍA SÁNCHEZ, este movimiento permitió dar a conocer «los abusos/agresiones hacia las mujeres» y a «tomar conciencia de la necesidad de persecución de los agresores y protección hacia las víctimas»[49]. Tanto es así que el Parlamento Europeo celebró una reunión en respuesta a esta campaña, donde expresó su apoyo, aplaudiendo a los millones de personas que compartieron públicamente sus historias de violencia sexual en busca de justicia y para romper el silencio. Del mismo modo, instó a los Estados miembros a redactar y aplicar leyes y políticas que abordaran la violencia y el acoso sexual, promoviendo cambios para poner fin a la violencia sexual, ayudar a las víctimas y afrontar las

---

[48] ONU. *Un momento transformador, liberador y empoderador*, *2018.* Disponible en: https://acnudh.org/me-too-un-momento-transformador-liberador-y-empoderador/

[49] SÁNCHEZ GARCÍA, B.; «La nueva concepción de la libertad sexual en la ley del "solo sí es sí" y su problemática aplicación retroactiva», *Revista de Derecho Penal y Criminología*, 2023, n.º 30, pp. 117-118.

consecuencias perjudiciales que este tipo de violencia genera en la sociedad. Como resultado de esta sesión europea, aumentaron las denuncias por acoso sexual en el Parlamento[50].

En España, se han activado movilizaciones a través de las redes sociales para denunciar diversas problemáticas relacionadas con la violencia de género y la defensa de los derechos de las mujeres. Por ejemplo, el movimiento «*Ni Una Menos*» se ha centrado en denunciar los asesinatos machistas, mientras que el «*Tren de la Libertad*» ha defendido los derechos sexuales y reproductivos de las mujeres. Asimismo, con motivo del Día Internacional de la Mujer, el 8 de marzo, se llamó a la movilización en 2018 a miles de mujeres a participar en una huelga feminista, con manifestaciones multitudinarias e históricas en todo el país. El caso de la agresión sexual múltiple de «la Manada», durante las fiestas de San Fermín de 2016, provocó un fuerte debate en la sociedad española sobre la cultura de la violación, la victimización de las mujeres y la necesidad de una reforma en las leyes relacionadas con los delitos sexuales. Como respuesta a la sentencia dictada en este procedimiento, y a la situación de impunidad percibida por muchas mujeres, surgió la campaña «*Yo sí te creo, hermana*», que a través de la red se extendió rápidamente. Numerosas mujeres compartieron sus testimonios y experiencias y se organizaron concentraciones y protestas en toda España para pedir un cambio fundamental en la forma en que la sociedad y las instituciones afronten estos casos[51]. Recientemente, se utilizó otra etiqueta en apoyo a una futbolista de la selección española y con la condena social rotunda por un beso no consentido del presidente de la Real Federación Española de Fútbol, bajo el lema *«Se acabó»,* reivindicando un deporte libre de violencias machistas y en apoyo a las campeonas del mundo.

Por lo tanto, se puede afirmar que también hay una cara positiva en el uso de la tecnología y la comunicación y relación en el ciberespacio.

5. UTILIZACIÓN DE LAS TECNOLOGÍAS COMO MEDIO DE CONTROL

A pesar de que la digitalización ha traído consigo importantes avances en términos de visibilidad, organización, reivindicación y reconocimiento de los derechos de las mujeres y las niñas, también ha facilitado la materialización de la violencia contra ellas a través de las nuevas tecnologías[52]. El abuso hacia las mujeres y niñas ha encontrado en Internet un medio idóneo para ejercer control, dominio y abuso.

Antes de la tecnología digital, las agresiones tenían un alcance territorial limitado al entorno en el que se producían. Sin embargo, Internet se ha convertido en una autopista que posibilita el intercambio y el tráfico de imágenes ilegales, información y actividades de espionaje.

Las características del medio en el que se cometen los delitos tecnológicos favorecen a los agresores, que aprovechan factores tales como el anonimato, la rapidez en la transmisión de los contenidos,

---

50 *Ibidem.*

51 EURONEWS & EFE. «España aprueba la ley del 'solo sí es sí'», *EURONEWS,* 26 de agosto de 2022. Disponible en: https://es.euronews.com/2022/08/26/espana-aprueba-la-ley-del-solo-si-es-si

52 ARÁNGUEZ SÁNCHEZ, T., OLARIU, O.; «Feminismo digital. Violencia contra las mujeres y brecha sexista en Internet», Dykinson, 2021. Disponible en: https://repositorio.comillas.edu/rest/bitstreams/484918/retrieve

la inmediatez, la viralidad y la dificultad en la persecución y la prueba para facilitar su impunidad y acrecentar la lesión de los bienes jurídicos comprometidos. Estos rasgos derivan, esencialmente, de las características de elasticidad en el tiempo y la contracción del espacio que conforma lo que se ha venido a llamar «*la arquitectura del ciberespacio*». Es decir, tienen que ver con el lugar donde se comete el delito. La distancia deja de ser un obstáculo para la comunicación, pues la distancia física no tiene relevancia en Internet. El tiempo también cambia en Internet: su percepción social y su organización[53].

Además, lleva a la constatación de otras características asociadas a la deslocalización de Internet (como son las cuestiones de transnacionalidad, la no centralización y la neutralidad), que conduce a la posibilidad de trasladarse de un lugar a otro en el ciberespacio sin fronteras y sin censuras[54].

Junto a ello, la escasa o nula regulación sobre la veracidad de los datos proporcionados al crear un perfil en la mayoría de las redes sociales permite que personas mayores de edad accedan a plataformas destinadas a menores, así como que algunos menores falsifiquen su información para ingresar en las redes sociales o en los sitios web pornográficos, con el riesgo implícito de ser objeto de acoso, abuso o acceso a contenidos inadecuados para su edad.

El Instituto Europeo de la Igualdad de Género (EIGE), en el informe de 2022[55], se centra en varias formas de ciberviolencia que han sido seleccionadas en atención a los resultados del mapeo nacional realizado en los 27 Estados miembros de la UE, que proporcionó una visión general de la prevalencia de la violencia cibernética en el territorio nacional y de la UE.

En este sentido, el informe europeo identifica una serie de campos en los que se desarrollan estas formas de violencia[56]:

1. Acecho (*cyberstalking*). Se produce de forma metódica y persistente y lo perpetra una persona con la intención de socavar la sensación de seguridad de la víctima. Implica el uso de correos electrónicos, mensajes ofensivos o amenazantes, la difusión de fotos o vídeos íntimos y el seguimiento de las víctimas por diversos medios. El ciberacoso es una manifestación del acoso que se caracteriza por el ámbito espacial en el que se produce (TIC), así como por su versatilidad, porque puede albergar distintas formas de acoso: sexual, religioso, racial … y también en el ámbito de la violencia de género.
2. Intimidación, coacciones y acoso (*cyberharassment-bullying*). También es una conducta persistente diseñada para causar angustia emocional severa y, a menudo, miedo a daños físicos.

---

[53] Entre otros, AGUSTINA SANLLEHI, J.R.; «La arquitectura digital de Internet como factor criminógeno: Estrategias de prevención frente a la delincuencia virtual», *International e-Journal of Criminal Science,* 2009, n.º 3, y MIRÓ LLINARES, F.; «El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio», Madrid, Marcial Pons, 2012. pp. 148-157.

[54] ALCÁNTARA, J.; «La neutralidad de la Red y porqué es una mala idea acabar con ella», Biblioteca de las Indias, Madrid, 2011, pp. 10 y ss.

[55] EIGE. Índice de Igualdad de Género, 2022. Disponible en: https://eige.europa.eu/gender-equality-index/2023

[56] *Ibidem.*

Las principales víctimas son jóvenes y menores con vulnerabilidad. Puede implicar solicitudes de favores sexuales o la entrega de cualquier contenido no deseado que se considere ofensivo, humillante, degradante o intimidante con amenazas y discursos de odio en redes.

3. Discurso de odio en línea basado en el género. Odio (*Online gender-based hate speech*). Aunque es un término amplio vinculado a la violencia contra grupos por sus condiciones étnicas, religiosas o de origen, también se registra contra las mujeres e implica sexualización, cosificación y comentarios degradantes sobre el aspecto físico, así como amenazas de violación.
4. Difusión no consentida de imágenes íntimas. (*Non-consensual intimate image abuse*). El espionaje digital es otra forma de violencia en la que los perpetradores toman imágenes no consensuadas ni consentidas de zonas íntimas de la mujer y las comparten o envían fotografías explícitas no solicitadas de ellos mismos. Aclarar que la difusión no consentida de imágenes se refiere a la acción de compartir o distribuir imágenes de una persona sin su permiso, la toma no consentida de imágenes supone la captura de imágenes de una persona sin su conocimiento o autorización. Y, por último, la recepción no solicitada de imágenes explícitas implica recibir imágenes que contienen contenido sexual o explícito sin haberlo pedido.

Según el informe EIGE 2022, durante el mapeo se detectaron otras formas de violencia cibernética como, por ejemplo, las siguientes[57]:

1. Troleo. El Diccionario de la Real Academia Española[58] aporta una definición precisa: «*En foros de internet y redes sociales, publicar mensajes provocativos, ofensivos o fuera de lugar con el fin de boicotear algo o a alguien, o entorpecer la conversación». Empieza a considerarse una forma de acoso el incluir mensajes agresivos o confusos. El perpetrador puede no tener relación con las víctimas y sus armas. Cuando el troleo es sexista, son insultos basados en el género, o se utiliza un lenguaje impúdico y amenazas de violación y muerte por parte de un grupo coordinado para humillar a las mujeres, particularmente a aquellas que expresan su opinión*».
2. Incendiarios (*Flameo*). Es una forma de comunicación en línea agresiva y hostil que siempre se caracteriza por contener insultos, desafecto y odio. Tipográficamente, sus mensajes suelen contener letras mayúsculas y signos de exclamación. Se usa para provocar la reacción de otro usuario. Está muy relacionada con el troleo y en pocas legislaciones o políticas se incluyen como forma de violencia. Estas acciones pueden ser abiertamente misóginas y, a menudo, contienen amenazas o fantasías de violencia sexual o incitación a la misma.
3. Revelación de datos (*Doxing o doxxing*). Consiste en buscar, recopilar y compartir públicamente información de identificación personal en contra de la voluntad del objetivo. Incluye datos personales y sensibles, como domicilio, fotografías y nombres de la víctima y familiares. Puede ser utilizada por un gran número de perpetradores en campañas de acoso y amenazas con consecuencias psicológicas significativas y, al permitir localizar físicamente a las víctimas,

---

57 *Ibidem.*

58 Diccionario de la lengua española de la RAE, actualización 2023. Disponible en: https://dle.rae.es/trolear

también puede ser un precursor de la violencia física. Los métodos empleados para adquirir dicha información incluyen la búsqueda en bases de datos disponibles públicamente y sitios web de redes sociales, así como la piratería y la ingeniería social. Los motivos pueden ser el acoso, la exposición, el daño financiero, la extorsión e incluso el señalamiento de la víctima en el mundo físico. También puede implicar la manipulación de esta información con la intención de exponer y avergonzar aún más a la víctima.

4. Violencia a través de los dispositivos conectados (*IoT-facilitated violence*). Es la explotación del IoT (Internet de las cosas o dispositivos conectados) para acosar, acechar, controlar o abusar. Se lleva a cabo a través de aparatos como timbres inteligentes, altavoces, cámaras de seguridad o cualquier otro dispositivo conectado a Internet y con control remoto. Algunos ejemplos de este tipo de violencia son accionar interruptores a distancia (como los de las luces o la calefacción del hogar de la víctima), encerrar a la víctima controlando el sistema de seguridad inteligente o grabar audios o vídeos de esta de su vida privada mediante cámaras de seguridad o dispositivos particulares.

Sin embargo, según este informe de EIGE, es importante considerar que estas formas de agresión se refieren a las acciones y comportamientos en términos generales, para señalar formas de violencia que podrían no ser consideradas como delitos en los diferentes Estados miembros, o entenderlas como incluidas dentro de otras figuras delictivas. Por eso resulta tan importante la aprobación de la Directiva (UE) 2024/1385 sobre la lucha contra la violencia contra las mujeres y la violencia doméstica.

5.1. *Marco general: violencia digital contra mujeres y niñas*

5.1.1. Manifestaciones

La violencia digital dirigida al colectivo de mujeres y niñas en su conjunto se manifiesta de distintas formas, como son: discurso de odio, difusión de mensajes falsos y cosificación de las mujeres[59].

En cuanto a los discursos de odio, estos se difunden en redes sociales o páginas *web* predominantemente misóginas, donde se promueve la denigración de la mujer, acogiéndose al derecho a la libertad de expresión. Estas disertaciones tienden a ridiculizar a las mujeres en contextos que tradicionalmente han sido dominados por hombres, como la política, los deportes o las empresas.

Por su parte, la difusión de mensajes falsos o información manipulada tiene el objetivo de anular o disminuir la validez de las opiniones expresadas por las mujeres. La divulgación de este tipo de difamación por conducto de medios digitales puede alcanzar a diversos sectores en poco tiempo, con un bajo costo y esfuerzo. Además, la distancia física entre el agresor y la víctima facilita la desinhibición de conductas inapropiadas. Resalta la facilidad con la que se pueden crear perfiles falsos en el entorno digital, lo que permite la invisibilidad de los agresores y genera una sensación de impunidad.

---

[59] OEA/CICTE y OEA/CIM/MESECVI. *La violencia de género en línea contra las mujeres y niñas*. *Guía de conceptos básicos*, 2023. Disponible en: https://www.oas.org/es/sms/cicte/docs/Guia-conceptos-basicos-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

Con respecto a la cosificación de las mujeres, se ve potenciada y favorecida por la manera en que son simbolizadas en los medios de comunicación, los videojuegos, la música, la publicidad, las series y la moda. Estas representaciones perpetúan estereotipos de género y presentan a las mujeres y niñas como meros objetos de deseo sexual. Esto contribuye a la normalización de ciertas conductas que sostienen las estructuras patriarcales presentes en el mundo analógico. Esta configuración estereotipada aumenta la presión social ejercida sobre todas las mujeres, pero, especialmente, sobre las adolescentes y las niñas, que son más influenciables debido a su menor grado de madurez, quedando expuestas a una imagen irreal de perfección, a la perpetuación de mitos sobre el amor romántico y a la idealización de las relaciones de pareja. En este sentido, se ha pronunciado el Consejo de Europa en diferentes documentos, entre los que debemos destacar *La Estrategia de Igualdad de Género* 2018-2023[60], donde se señala que:

> «*Los medios de comunicación y las redes sociales desempeñan un papel importante en nuestras vidas, en especial, cuando se utilizan para intercambiar información y concienciar más sobre una serie de cuestiones. Sin embargo, también ha quedado demostrado que las redes sociales, en concreto, son objeto de uso abusivo y que, a menudo, mujeres y niñas sufren amenazas violentas y sexualizadas en la red. Las redes sociales y los videojuegos figuran entre las plataformas concretas que actúan como transmisores de la incitación sexista al odio. Con frecuencia, la libertad de expresión se desvirtúa como excusa para amparar conductas inaceptables y ofensivas. Al igual que sucede con otras formas de violencia contra la mujer, sigue sin denunciarse la incitación sexista al odio, pero sus efectos para la mujer, ya sean emocionales, psicológicos o físicos, pueden ser desoladores, en especial, para las chicas y mujeres jóvenes. Con el sexismo sucede lo mismo», teniendo por objeto «crear alianzas con las partes interesadas oportunas para poner coto a la pornografía violenta y degradante en Internet, a la vista de su influencia negativa en las relaciones de género, a las prácticas sexuales dañinas y a la coacción*».

5.1.2. Estereotipos, cosificación, perpetuación de roles y micromachismo

Para analizar la presencia de estereotipos que fomentan la discriminación de las mujeres, debemos comenzar definiendo el concepto de género. Tradicionalmente, los conceptos de género y sexo fundamentan los derechos de las mujeres y de las minorías sexuales.

En primer lugar, el concepto de género se sustenta no en una condición biológica sino en una construcción puramente social. La idea de género se construye por la atribución de una serie de roles, expectativas, comportamientos e incluso estereotipos que se estiman erróneamente, propios del hombre y de la mujer. Para MARTÍNEZ DE PISÓN CAVERO[61], la construcción social del género comprende, entre otras, características culturales, sociales, políticas y psicológicas. De la definición de género como constructo social nacen los roles y estereotipos que se atribuyen tanto a los hombres como a las mujeres y

---

[60] ESPAÑA. *Consejo de Europa Estrategia de Igualdad de Género 2018-2023*, 2018. Disponible en: https://rm.coe.int/estrategia-de-igualdad-de-genero-del-coe-es-msg/16808ac960Una

[61] MARTÍNEZ DE PISÓN CAVERO, J. M.; «La identidad de género en el Tribunal Europeo de Derechos Humanos». *Anuario de filosofía del derecho*, 2022, n.º 38, pp. 105-136

que, sin duda, inciden en la discriminación. Ello es debido, fundamentalmente, a que dichos roles y estereotipos se han creado sobre la base de una construcción histórica de discriminación y reparto de papeles bajo creencias y estructuras patriarcales. Con este punto de partida, se formulan los conceptos de sexo (entendido como condición biológica) y género (como constructo social)[62].

En segundo lugar, una vez conocido el origen de los roles y estereotipos de género, procede analizar este último concepto. La definición que establece el Alto Comisionado de los Derechos Humanos de la ONU determina lo siguiente:

> «*Un estereotipo de género es una visión generalizada o una idea preconcebida sobre los atributos o las características, o los papeles que poseen o deberían poseer o desempeñar las mujeres y los hombres*»[63].

Es importante destacar la conexión existente entre la presencia de estereotipos de género y los actos de violencia que sufren las mujeres. Así se manifiesta el Alto Comisionado de los Derechos Humanos, que establece que los estereotipos de género agravados impactan de forma desproporcionada en las mujeres y en las niñas[64].

El peligro de los estereotipos radica en que la sola pertenencia a un grupo como mujer o como hombre implica atribuir unas ciertas características o roles específicos. Y ello supone que, de no cumplirse las actitudes, atributos o características que se corresponden con el sexo biológico según la designación patriarcal, la persona va a sentirse rechazada, discriminada e incluso excluida de la comunidad o del grupo social. Nos referimos a atributos como, por ejemplo, los relativos al físico de una persona que no encaje con los cánones o estereotipos que ha establecido un determinado grupo social sobre la apariencia que debe de tener una mujer o un hombre (ya sea por altura, por delgadez o por cualquier elemento o característica física que se aleje de los patrones impuestos). Ello lleva a destacar dos elementos: el primero de ellos, es la arbitrariedad de los estereotipos y, el segundo, el impacto o consecuencia de discriminación y exclusión de la persona si no los cumple. Cada grupo social establece sus propios roles y estereotipos que difieren unos de otros y no tienen por qué ser idénticos. Así, por ejemplo, un grupo social determinado en un ámbito urbano puede tener unos hábitos o costumbres que en un municipio rural no se exigen y viceversa.

La consecuencia de los estereotipos y roles es, precisamente, que algunos son dañinos para las personas y vulneran sus derechos, en particular, los derechos de las mujeres y las niñas. El Alto Comisionado determina la existencia de algunos estereotipos considerados ilícitos e indica una serie de ejemplos como: permitir la violencia conyugal como consecuencia de una discriminación de la mujer relegada a la subordinación respecto del hombre, o no criminalizar la violencia sexual sufrida por las mujeres y niñas[65]. También se incluyen, entre otros, permitir los matrimonios forzados, prohibir a las mujeres

---

62 *Ibidem.*

63 ONU. *Estereotipos de género. El ACNUDH y los derechos humanos de las mujeres y la igualdad de género,* Informe 2021. Disponible en: https://www.ohchr.org/es/reports

64 *Ibidem.*

65 *Ibidem.*

el acceso a la educación, penalizar el adulterio, etc. Los ejemplos anteriores ponen de manifiesto una vulneración de los derechos de las mujeres y niñas, al mismo tiempo que normalizan la violencia y perpetúan su cosificación.

En la Unión Europea se han producido grandes avances, si bien quedan todavía cosas por hacer para conseguir la igualdad efectiva entre hombres y mujeres y evitar las vulneraciones sistemáticas de derechos a las que se ven sometidas, como pueden ser la violencia y la pobreza. Desde el punto de vista social, como consecuencia del establecimiento de una normativa protectora de las mujeres, se ha alcanzado un consenso en la lucha frente a prácticas culturales, actitudes y violaciones de derechos de las mujeres y niñas[66]. Los estereotipos también fomentan una cosificación de la mujer, pudiendo encontrarlos en multitud de ámbitos, como la música, el cine, la publicidad, los medios de comunicación y las redes sociales. Así, transmiten unos cánones de belleza y de imagen que, de no cumplir con los previos modelos fijados, pueden dar lugar a actitudes de rechazo y discriminación junto a la exclusión social, además de trastornos alimentarios, incitación al suicidio, actitudes homófobas y similares.

Al respecto, el artículo 5 de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer[67], nos indica el deber de los Estados de establecer medidas para luchar contra los estereotipos relacionados con el género que son los que perpetúan la discriminación de la mujer respecto del hombre. Así, se establece en su artículo 5 lo siguiente:

> «*Los Estados Partes tomarán todas las medidas apropiadas para: a) Modificar los patrones socioculturales de conducta de hombres y mujeres, con miras a alcanzar la eliminación de los prejuicios y las prácticas consuetudinarias y de cualquier otra índole que estén basados en la idea de la inferioridad o superioridad de cualquiera de los sexos o en funciones estereotipadas de hombres y mujeres*».

De igual forma, entre los objetivos fundamentales de *La Estrategia de Igualdad de Género 2020-2025* de la UE se encuentra poner fin a la violencia de género y combatir los estereotipos de género. Ello se desprende de cuando señala que:

> «*La violencia en línea dirigida a las mujeres ha proliferado, con consecuencias concretas alarmantes. Esto es inaceptable. Supone un obstáculo a la participación de las mujeres en la vida pública. El acoso, la intimidación y los insultos en las redes sociales tienen repercusiones profundas en la vida cotidiana de las mujeres y las niñas. La Comisión propondrá la norma de servicios digitales para esclarecer las responsabilidades de las plataformas en línea con respecto a los contenidos difundidos por los usuarios. La norma de servicios digitales aclarará qué medidas se espera que apliquen las plataformas a la hora de atajar las actividades ilícitas*

---

[66] DÍEZ PERALTA, E.; «Los derechos de la mujer en el Derecho internacional», *Revista española de derecho internacional*, 2011, v. 63, n.º 2, pp. 87-121.

[67] BOE. *Instrumento de Ratificación de 16 de diciembre de 1983 de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer, hecha en Nueva York el 18 de diciembre de 1979*. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-1984-6749

en línea, al tiempo que protegen los derechos fundamentales. Los usuarios también tienen que ser capaces de actuar ante otros tipos de contenidos abusivos y nocivos, que no siempre se consideran ilícitos pero que pueden tener consecuencias devastadoras. Con objeto de proteger la seguridad en línea de las mujeres, la Comisión facilitará el desarrollo de un nuevo marco de cooperación entre las plataformas de internet»[68].

Por otra parte, también existe un tipo de machismo que, debido a su menor grado de intensidad, no resulta mortal y pasa desapercibido, pero que se encuentra arraigado en nuestra cotidianidad y, lamentablemente, es aceptado. Es el denominado «micromachismo»[69].

Esta idea se refiere a formas sutiles y, a menudo inconscientes, de sexismo o discriminación de género, que pueden ocurrir en las interacciones y comportamientos cotidianos. Estas acciones pueden parecer triviales o menores, pero su efecto acumulativo implica la contribución a la perpetuación de los roles y estereotipos de género tradicionales, que pueden socavar la igualdad y la autonomía de las mujeres, contribuyendo a la perpetuación de las desigualdades entre hombres y mujeres. Estas conductas se pueden dar dentro de las relaciones personales, entornos profesionales y estructuras sociales.

De igual forma, estos micromachismos son reproducidos en las redes sociales y foros de debate en red. Este tipo de actitudes contribuyen a silenciar a las mujeres, haciendo que sus problemas y denuncias no sean tomados en serio. Asimismo, la desvalorización de su trabajo en redes sociales se manifiesta a través de la falta de reconocimiento, de remuneración económica insuficiente y de la presencia de estereotipos de género limitantes. Algunos ejemplos, serían: si un hombre cuestiona el conocimiento de una mujer e intenta ilustrar su discurso (*mansplaining*), hacerle creer sutilmente a una mujer que está loca (*gaslighting*) o cuando una mujer tiene una idea la desarrolla y el hombre se lleva los méritos, lo que se conoce como apropiación machista de ideas (*bropiating*).

En conclusión, para evitar estas actitudes en el ámbito virtual es fundamental abordar y prevenir la normalización de la violencia machista en línea en la adolescencia. Igualmente, educar a la juventud en la igualdad de género, promover entre los y las jóvenes relaciones saludables y respetuosas y fomentar una cultura de rechazo a cualquier forma de violencia. En idéntico sentido, trabajar en la concienciación y el cambio de actitudes y comportamientos en la sociedad en general.

5.2. *Marco individual: violencia digital contra mujeres y niñas*

En la esfera digital, las agresiones dirigidas a cada mujer de manera individual son diversas, al igual que los instrumentos utilizados para llevarlas a cabo. Además, la distancia física entre el agresor y la víctima facilita la desinhibición de comportamientos inapropiados. Como manifestaciones de las mismas se pueden mencionar las siguientes:

---

[68] ONU. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de la UE sobre los derechos de las víctimas (2020-2025),* 2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020DC0258

[69] BONINO MÉNDEZ, L.; «Los micromachismos», *Revista La Cibeles,* n.º 2, 4.

1. Registro de movimiento e información de ubicación y escucha, con la instalación de recursos de geolocalización o dispositivos espías, como cámaras IP o grabadoras de sonido con conexión a Internet. Estas herramientas, que son de fácil implementación e incluso accesibles de forma gratuita, permiten conocer los movimientos y la ubicación exacta de la víctima en todo momento. Además, mediante el uso de *software* específico, pueden acceder a la lectura de mensajes instantáneos y archivos multimedia descargados por la persona vigilada, lo que facilita el hostigamiento y la amenaza constante y genera en la víctima una sensación de vigilancia permanente.

2. Robo de datos y suplantación de identidad con el objetivo de desprestigiarlas tanto en el ámbito público como en el privado, con el fin de destruir o influir en su entorno más cercano, incluyendo en el mismo amistades, familiares y relaciones laborales. Estas acciones generan situaciones de ansiedad, acoso y aislamiento. Además, es importante resaltar el esfuerzo y el desgaste físico y mental que conlleva para las víctimas la retirada de los contenidos difamatorios, los cuales las exponen ante la opinión pública. En muchos casos, estas acciones afectan a la imagen que se proyecta, ya que contar con una referencia digital negativa puede tener repercusiones, por ejemplo, en el acceso a un empleo.

3. Generar situaciones de amenaza constante, agresión, difamación y/o extorsión, que incluyen la emisión de numerosas llamadas y mensajes, la elaboración de vídeos o imágenes de contenido privado con el chantaje de su publicación, el envío de contenidos de carácter sexual, violento o lascivo sin el consentimiento de la víctima, y la obtención de contraseñas de cuentas mediante coerción, u otras formas abusivas o defraudatorias utilizadas por los acosadores.

   Es preocupante que los acosadores puedan acceder a la víctima en cualquier momento del día o de la noche, y desde cualquier lugar, lo que provoca una invasión en su espacio personal, incluso en entornos que se consideran seguros, como su propio hogar.

4. Grabación de agresiones sexuales y posterior divulgación, generando una doble victimización para la persona afectada. En primer lugar, se produce la agresión física en sí misma, lo cual ya genera un profundo impacto emocional y, en segundo lugar, la difusión masiva y constante de estas grabaciones y el intercambio de imágenes a través de los diferentes dispositivos digitales, con lo que esto conlleva para la víctima, que experimenta sentimientos de culpa, vergüenza y una humillación constante. Una vez que los contenidos se comparten en redes sociales y aplicaciones de mensajería instantánea, escapan al control de la víctima, y de los agresores, lo que genera un estado constante de inseguridad e indefensión. La falta de conocimiento sobre quién ha tenido acceso a la publicación y la posibilidad de que sea duplicada, difundida, revelada o reproducida plantean incertidumbre.

El Observatorio Español de Delitos Informáticos (OEDI) publicó en 2022 el artículo *Estudio y evolución de la violencia de género digital en la atención temprana a las víctimas*[70]. En este artículo, afianzando las

[70] SAMPER, S., RAYA, G.; «Estudio y evolución de la violencia de género digital en la atención temprana a las víctimas», *Libro de actas, XIV Congreso (inter)nacional de psicología jurídica y forense,* 2022, pp. 389-391.

manifestaciones contenidas en párrafos anteriores, se pone de manifiesto que el 89 % de los agresores tienen el control de las víctimas, accediendo o administrando sus cuentas. En cuanto a la frecuencia con la que se produce la violencia de género digital, se afirma que esta aparece principalmente a diario (70 %) y a cualquier hora (95 %). Esto es, se puede llegar a sufrir las 24 horas del día, durante los 7 días de la semana, por la propia naturaleza del ciberespacio. En un 64 % de los casos, los agresores han accedido al teléfono de la víctima y a sus contenidos[71]. En el supuesto de que la víctima impidiera el acceso a su teléfono móvil, un 67 % de los agresores se enfadaban. Un 75 % de las víctimas bloquearon al agresor en sus teléfonos móviles y redes sociales. Esta acción no pudo impedir el acoso de su agresor, ya que el 89 % de los victimarios buscaron fórmulas alternativas para seguir contactando, empleando números de teléfonos alternativos o utilizando otros perfiles en redes sociales y aplicaciones de mensajería instantánea[72].

A pesar de que en las redes sociales se encuentran disponibles herramientas de protección para las víctimas, como el bloqueo del agresor, la posibilidad de presentar denuncias o las prohibiciones de retuiteo y etiquetado, o el cierre de perfiles, se considera que estos mecanismos son insuficientes para la protección de los derechos de las víctimas debido a la facilidad con la que los agresores pueden abrir un nuevo perfil y continuar con el acoso inflingido.

6. INTELIGENCIA ARTIFICIAL

Una de las consecuencias de la evolución de las nuevas tecnologías es la aparición de la inteligencia artificial, conocida por sus siglas IA. La IA, como apuntó el Parlamento Europeo, es la destreza de una máquina de imitar y replicar las mismas capacidades del ser humano, como el razonamiento, el aprendizaje, la creatividad, la capacidad de idear y la toma de decisiones. Esta tecnología se basa en un sistema de algoritmos complejos y emplea grandes cantidades de datos e información para realizar tareas[73]. Esto permite que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con un fin específico. La máquina recibe datos, los procesa y responde a ellos, mediante el aprendizaje automático con capacidad para aprender sin ser programada.

La IA no es de reciente creación, sino que ya en la década de los años 40 y 50 se establecieron los primeros trabajos en la teoría de los sistemas y la computación. En los últimos años, se ha producido una expansión y desarrollo de las técnicas de implementación que ha afectado a todos los ámbitos: trabajo, ocio, cultura, arte, etc., incluidos la comisión de delitos y la prevención de los mismos. En este sentido, el concepto, la clasificación y la regulación de los sistemas de inteligencia artificial se encuentran en plena evolución.

Disponible en: http://sepjf.org/wp-content/uploads/2019/03/LIBRO-DE-ACTAS_XIV-CONGRESO-INTERNACIONAL-DE-PSICOLOG%C3%8DA-JUR%C3%8DDICA-Y-FORENSE.pdf

71 *Ibidem.*

72 *Ibidem.*

73 PARLAMENTO EUROPEO. *Ley de IA de la UE: primera normativa sobre inteligencia artificial*, 2023. Disponible en: https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial

En los últimos años, su avance ha sido tan exponencial que ha requerido de una regulación específica ante el peligro que pueden llegar a correr nuestros derechos y garantías. Por ello, la Unión Europea comenzó a elaborar varias propuestas de desarrollo para dar una respuesta a la necesidad de establecer límites a su uso en aras de la protección y seguridad de las personas.

En este sentido, destaca el *Libro Blanco sobre la Inteligencia Artificial. Un enfoque europeo orientado a la excelencia y la confianza* (2020) de la Comisión Europea[74] y el reciente Reglamento de Inteligencia Artificial (2024) del Parlamento Europeo y del Consejo.

Como todo, la IA tiene sus ventajas y desventajas. En cuanto a los beneficios, entre otros, se encuentran los siguientes: asistencia en la toma de decisiones, automatización de tareas, personalización de experiencia, ayudar en la lucha contra ciberataques y otras amenazas en línea, reconocer patrones e impedir ataques, detección de noticias falsas y desinformación. Pero también cuenta con sus problemas e inconvenientes, entre ellos: la presencia de sesgos y discriminación, vulneración de la seguridad y privacidad, ausencia de controles, dependencia tecnológica, costes elevados y falta de transparencia.

Con referencia a la preocupación de sesgo y discriminación, efectivamente, la IA puede aplicar sesgos discriminatorios, bien por el origen racial en cuanto a las diferencias de aspecto entre las personas, o bien por perpetuar los relacionados con el género que afectan, sin duda, a los derechos de las mujeres y las niñas. Por ello, es fundamental reconocer y corregir estos prejuicios de género en la inteligencia artificial para asegurar la igualdad, lo que sólo se puede conseguir corrigiéndolo en la sociedad y en las personas que intervienen en el proceso creativo y de aprendizaje, puesto que esta tecnología replica los sesgos de quienes la crean. Así se demuestra que si aplicamos, por ejemplo, la IA para la selección de altos puestos de dirección, se seleccionará preferentemente de forma discriminatoria a un hombre, por el número de varones presentes en los cargos más altos directivos, porque el sistema tomará los datos de la sociedad, no solamente valorará CV del candidato/a, por el fenómeno denominado techo de cristal[75]. Debemos tener presente que si los sistemas tecnológicos y algorítmicos no están bien diseñados y estructurados, pueden generar resultados discriminatorios, contribuyendo así a aumentar las desigualdades existentes[76].

Otra de las preocupaciones es la seguridad y privacidad de sus sistemas. Así lo revela el *Informe 2024 Consumer Cybersecurity Assessment*[77], que muestra que, de los países analizados (España, Australia, Francia, Alemania, Italia, Reino Unido y EE. UU.), un 67 % de las personas expresan su inquietud por este problema y en España, específicamente el 80 %.

---

[74] UE. *LIBRO BLANCO sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*, 2020. Disponible en: https://op.europa.eu/es/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

[75] YELA UCEDA, M.; «Análisis multidisciplinar sobre las posibles vulneraciones de derechos en el uso de la inteligencia artificial en el Derecho Penal», en ROPERO CARRASCO, J. (Coord.) «Aspectos jurídicos de actualidad en el ámbito del Derecho Digital», Tirant Lo Blanch, 2023, pp. 380-382.

[76] MIRÓ LLINARES, F.; «Cometer delitos en 140 caracteres: El derecho penal ante el odio y la radicalización en Internet», Madrid, *Marcial Pons*, 2017, pp. 10-12

[77] BIFDEFENDER. *2024 Consumer Cybersecurity Assessment Report*, 2024. Disponible en: https://blogapp.bitdefender.com/hotforsecurity/content/files/2024/03/Bitdefender-CSG-Report-creat7534-interactive.pdf

Por otro lado, el mal uso de generar imágenes y/o contenidos audiovisuales por IA protagonizadas mayoritariamente por mujeres y niñas suponen una vulneración de sus derechos y contra su integridad. Así lo destaca la reciente investigación de la empresa de ciberseguridad *HomeSecurity Heroes*, titulada *«State of deepfakes 2023»*[78]. Este estudio resalta que, de una muestra compuesta por los 10 sitios *web* más relevantes dedicados a la pornografía *deepfake* y 85 canales en plataformas como *YouTube, Vimeo* y *Dailymotion*, el 98 % de estos vídeos son de contenido pornográfico. Entre sus conclusiones se señala que la producción de vídeos falsificados con contenidos pornográficos no es equitativa, sino más bien discriminatoria. Este tipo de suplantación atenta contra la intimidad de los individuos; sin embargo, no impacta a todas las personas de la misma manera, ya que se observan sesgos de género evidentes: un 99 % de las víctimas son mujeres[79].

Otro ejemplo de un uso incorrecto de la IA son los sucesos ocurridos en Almendralejo (Badajoz) en 2023. En este caso, varios menores a través de una aplicación que utiliza IA (*ClothOff*), han intervenido en la creación de imágenes falsas de varias menores, utilizando su rostro y cuerpo para crear desnudos falsos virtuales que, sin duda, afectan a los derechos de las menores[80]. Por ello, los sistemas que aplican IA deben de respetar y preservar, como mínimo, los derechos humanos, porque a día de hoy partimos de la inexistencia de una IA autónoma y, por tanto, la responsabilidad recae bien en el diseño, bien en el uso que hagamos de la misma, sabiendo que en el caso de los desnudos falsos podemos vulnerar derechos tan esenciales como la libertad sexual, el honor o dignidad de la persona[81]. Estos acontecimientos desataron un debate sobre el control de las aplicaciones de IA y han supuesto una condena penal para los chicos que llevaron a cabo los actos. La dificultad para la sanción de estas conductas radica en determinar qué bienes jurídicos son lesionados y en qué posibles tipos penales cabría encajar este tipo de actos.

Fundamentalmente, este fenómeno *deepfake* infringe dos derechos: el derecho a la protección de datos y privacidad y el derecho a la intimidad, honor e imagen personal. La normativa de protección de datos es incumplida debido a la difusión de información que, aunque sea en gran medida falsa, utiliza datos personales auténticos, como el rostro o incluso la voz de una persona, lo que frecuentemente resulta en un tratamiento de datos sin el consentimiento de la persona afectada. Sobre este punto se han pronunciado varios autores, como DEVÍS MATAMOROS[82], quien afirma, conforme a la Sentencia

---

78 SECURITY HERO. *State of deepfakes*, 2023. Disponible en: https://www.securityhero.io/state-of-deepfakes/#key-findings:~:text=99%25%20of%20deepfake,the%20content%20features%20men

79 *Ibidem.*

80 PALOMO, R.; «Un año de libertad vigilada para 15 menores de Almendralejo por manipular imágenes de niñas», *El País*, 9 de julio de 2024. Disponible en: https://elpais.com/sociedad/2024-07-09/un-ano-de-libertad-vigilada-para-15-menores-de-almendralejo-por-manipular-imagenes-de-ninas.html

81 YELA UCEDA, M.; «Oportunidades y potenciales riesgos de la aplicación de la inteligencia artificial en herramientas para la prevención de delitos», en JIMÉNEZ GARCÍA, F., y SÁNCHEZ GARCÍA, B.; «La atribución de una responsabilidad jurídico penal e internacional de la Inteligencia Artificial», Iustel, 2023, pp. 150-151.

82 DEVÍS MATAMOROS, A.; «Algunas claves del castigo penal del deepfake de naturaleza sexual», ibericonnect.blog, 2023. Disponible en: https://www.ibericonnect.blog/2023/07/algunas-claves-del-castigo-penal-del-deepfake-de-naturaleza-sexual/

del Tribunal Supremo núm. 181/2023, de 15 de marzo, que, dado que la integridad moral se entiende como una expresión directa de la dignidad humana y la inviolabilidad de la persona, este podría ser el lugar sistemáticamente más adecuado para incluir el castigo de estas conductas. Recuérdese que la tutela de la integridad moral se traduce en la prohibición de cualquier uso instrumental de un individuo y el derecho a ser tratado como persona y no como un simple objeto. Desde esta perspectiva, se ha barajado la posibilidad de incluir estas conductas entre los delitos contra el honor (básicamente en relación con los delitos de injurias del artículo 208 CP)[83], como afirma la doctrina científica, entre los que castigan la práctica de tratos degradantes de los contemplados en el artículo 173.1 del Código Penal. DEVÍS MATAMOROS, reconoce que la opción más apropiada es enmarcarlos dentro de los delitos contra la integridad moral. En el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en entornos digitales, se plantea la tipificación de este tipo de acciones, como veremos más adelante, entre los delitos que atentan contra la integridad moral, en un nuevo artículo 173 bis[84]. El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial define categorías de riesgos en relación a la IA, clasificándolos como prohibidos, graves o muy graves. Pero, las *deepfakes* no son un sistema de IA prohibido, no siendo tampoco un sistema de riesgo. Únicamente, se impone una obligación de transparencia, excepcionando de este deber a aquellas creaciones consideradas artísticas, siendo esta excepción una posible vía de acceso para la inaplicación de la norma.

---

[83] Esta es la opción escogida por el Grupo parlamentario SUMAR en su Proposición de Ley Orgánica de regulación de las simulaciones de imágenes y voces de personas generadas por medio de la inteligencia artificial, de 13 de octubre de 2023. Disponible en: https://www.congreso.es/public_oficiales/L15/CONG/BOCG/B/BOCG-15-B-23-1.PDF

[84] El texto que está sometido en estos momentos a informe acoge un nuevo artículo 173 bis que dice: *«Se impondrá la pena de prisión de uno a dos años a quienes, sin autorización de la persona afectada y con ánimo de menoscabar su integridad moral, difundan, exhiban o cedan su imagen corporal o audio de voz generada, modificada o recreada mediante sistemas automatizados, software, algoritmos, inteligencia artificial o cualquier otra tecnología, de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorias. Se aplicará la pena en su mitad superior si dicho material ultrafalsificado se difunde a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías, de modo que aquel se hiciera accesible a un elevado número de personas en el espacio virtual».* ESPAÑA, Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales. Disponible en: https://www.mpr.gob.es/servicios/participacion/Documents/ANTEPROYECTO%20DE%20LEY%20ORGÁNICA%20PARA%20LA%20PROTECCIÓN%20DE%20LAS%20PERSONAS%20MENORES%20DE%20EDAD%20EN%20LOS%20ENTORNOS%20DIGITALES.pdf

CAPÍTULO II.
MENORES Y ADOLESCENTES, INTERNET Y REDES SOCIALES

1. INFLUENCIA DE LAS REDES SOCIALES

Durante la etapa de la infancia y de la adolescencia, las personas se encuentran en una fase crucial de formación de su identidad y valores. En este periodo, tienen un papel relevante las redes sociales[85], influyendo en la visión y percepción de sí mismos, del mundo que los rodea y de su relación con los demás. Son plataformas que brindan oportunidades para establecer relaciones y mantenerse conectados con amigos y familiares, sitios donde las personas se encuentran y tienen la posibilidad de comunicarse, socializar e incluso formar lazos afectivos e íntimos, descubrir nuevas ideas e intereses y acceder de manera rápida e inmediata a información educativa y recursos útiles.

Sin embargo, el uso excesivo de las redes sociales puede afectar a la autoestima de las personas menores y de los y las adolescentes[86]. Al compararse con las imágenes y vídeos idealizados que ven en las redes sociales, pueden llegar a experimentar sentimientos de inseguridad y baja autoestima. Las publicaciones en redes sociales suelen mostrar una versión editada y cuidadosamente seleccionada de la vida de las personas, lo que puede llevar a que en la adolescencia exista una importante presión para cumplir con estándares irracionales y poco realistas de belleza y éxito. Los hombres son vistos como expertos en tecnología y videojuegos, se espera que sean agresivos y competitivos en los espacios en línea, son percibidos como menos emocionales y más racionales en sus interacciones y son vistos como más propensos a tener comportamientos irrespetuosos o abusivos en redes sociales.

Las redes sociales están llenas de imágenes de cuerpos perfectos y delgados que promueven los estándares de belleza irreales, imágenes eróticas, mostrando los cuerpos como si se tratase de meros objetos. En general, son las mujeres quienes en mayor medida tienden a compararse con estas imágenes y a sentirse insatisfechas con sus propios cuerpos, lo que puede llevar a comportamientos extremos de dieta y ejercicio, contribuyendo a trastornos alimenticios como la anorexia o la bulimia[87].

---

[85] Según el estudio *Adolescentes y redes sociales*, realizado por la Fundación de Ayuda contra la Drogadicción (FAD) y la Obra Social *«La Caixa»* en el año 2018, las redes sociales son utilizadas por los y las jóvenes principalmente para mantener el contacto con amigos y familiares, compartir fotos y vídeos, y estar al tanto de las novedades y eventos, como entretenimiento y para buscar información.

[86] De acuerdo con los datos proporcionados por el INE, se puede observar que los estudiantes son el grupo de personas que muestran mayor actividad en las redes sociales, con un 94,4 %, seguidos de cerca por los jóvenes de 16 a 24 años, con un 92,6 %. Estos grupos también demuestran una mayor confianza en las redes sociales, en comparación con los adultos mayores. INE. Datos estadísticos, 2024. Disponible en: https://www.ine.es/

[87] Es interesante destacar una investigación de *The Wall Street Journal* (septiembre 2021), con informes inéditos de *Facebook*, que concluye que *Instagram* es tóxica, sobre todo para las adolescentes. Revela que *«un 32 % de chicas dicen que cuando se sienten mal con su cuerpo, Instagram les hace sentir peor»*. Además, detalla el informe interno, denominado *Los archivos de Facebook,* que *«las comparaciones con lo que ven en Instagram pueden alterar el modo en que las jóvenes se perciben y describen a sí mismas»*. En 2019, *Facebook* había

Se asume que las mujeres están más interesadas en temas relacionados con la crianza de los hijos e hijas y el hogar, y se espera que compartan contenidos sobre esta temática. Se estereotipa a las mujeres como consumidoras ávidas de moda y tendencias, enfocándose en la ropa y los accesorios, y compartiendo constantemente este tipo de contenido; son asociadas con la promoción de estilos de vida saludables, la moda, la belleza y el bienestar, distorsionando la idea que tienen de ellas mismas y de las demás mujeres en cuanto el grado tan elevado de perfección física exigible para ser aceptables.

Ante la preocupación que estas situaciones generan, el legislador incluyó algunas referencias a delitos relacionados con la emisión de contenidos en redes, cuando pudieran afectar a las personas menores de edad. Así, la LO 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia, normativiza un concepto amplio de violencia[88] que ha sido criticada. Y ello porque, por un lado, constituye un elenco de conductas que, aunque pueda parecer que proporciona una completa protección a los intereses de las personas menores de edad, en realidad incurre en los mismos peligros que cualquier enumeración (dejar fuera algunas situaciones no contempladas, como, por ejemplo, la protección de la vida). Por otro lado, y desde la perspectiva de los límites al poder de castigar del Estado (entre otros, el cumplimiento del carácter de *ultima ratio* y del principio de proporcionalidad), la norma se presenta como una versión más de la expansión del Derecho penal, que puede colisionar con la naturaleza del Estado como garante de los derechos fundamentales de la ciudadanía. En el Preámbulo de la Ley, se justifica la creación de nuevos tipos penales (recogidos en los artículos 143 bis, 156 ter, 361 bis o 189 bis) 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. Se castiga a quienes, a través de estos medios, promuevan el suicidio, la autolesión o los trastornos alimenticios entre personas menores de edad, así como la comisión de delitos de naturaleza sexual contra estas*».

En relación con el bien jurídico protegido y su naturaleza, se trata de delitos de peligro, que el Consejo General del Poder Judicial, en su informe sobre el Anteproyecto, califica de peligro abstracto-concreto.

---

realizado otra investigación entre adolescentes estadounidenses y británicas, que reveló que más del 40 % de las jóvenes que se veían poco atractivas empezaron a sentirse así en *Instagram.* Sin embargo, a pesar de tener esta sensación, las adolescentes no dejan de usar la red. *«Se sienten adictas y saben que lo que ven es malo para su salud mental, pero se sienten incapaces de parar».*

88 En el artículo 1.2 de la LO 8/2021, se establece lo siguiente:
«*A los efectos de esta ley, se entiende por violencia toda acción, omisión o trato negligente que priva a las personas menores de edad de sus derechos y bienestar, que amenaza o interfiere su ordenado desarrollo físico, psíquico o social, con independencia de su forma y medio de comisión, incluida la realizada a través de las tecnologías de la información y la comunicación, especialmente la violencia digital. En cualquier caso, se entenderá por violencia el maltrato físico, psicológico o emocional, los castigos físicos, humillantes o degradantes, el descuido o trato negligente, las amenazas, injurias y calumnias, la explotación, incluyendo la violencia sexual, la corrupción, la pornografía infantil, la prostitución, el acoso escolar, el acoso sexual, el ciberacoso. La violencia de género, la mutilación genital, la trata de seres humanos con cualquier fin, el matrimonio forzado, el matrimonio infantil, el acceso no solicitado a pornografía, la extorsión sexual, la difusión pública de datos privados, así como la presencia de cualquier comportamiento violento en su ámbito familiar».*

Se castigan conductas de peligro para la vida o la salud, que afectan a sujetos pasivos especiales y que, como afirma LLORIA GARCÍA[89], *«no exige que se produzca el resultado buscado con la difusión de contenidos dañinos».*

Los tipos delictivos van desde la difusión pública a través de medios tecnológicos de contenidos específicamente destinados a promover, fomentar o incitar al suicidio de personas menores de edad o personas con discapacidad necesitadas de especial protección, que serán castigadas con penas de prisión de uno a cuatro años (artículo 143 bis del CP), hasta la difusión, por estos mismos medios y a los mismos sujetos pasivos, de contenidos específicamente destinados a promover, fomentar o incitar a la autolesión; en este caso, la pena será de prisión de seis meses a tres años. Por su parte, el artículo 189 bis, que ha sido modificado posteriormente conforme a la LO 4/2023, de 27 de abril[90], regula la conducta de distribución o difusión pública, también por los mismos medios tecnológicos, de contenidos específicamente destinados a promover, fomentar o incitar a la comisión de los delitos previstos en este capítulo y en los capítulos II y IV del presente título. En este caso, las penas serán de multa de seis a doce meses o pena de prisión de uno a tres años. Los capítulos referidos son los de las agresiones sexuales a menores de dieciséis años (cap. II), los delitos de exhibicionismo y provocación sexual (cap. IV) y el de los delitos relativos a la prostitución y a la explotación sexual y corrupción de menores (cap. V). Y, por último, el artículo 361 bis castiga la distribución o difusión pública, igualmente por los mismos medios tecnológicos, de contenidos específicamente destinados a promover o facilitar entre estas mismas personas menores de edad o personas con discapacidad necesitadas de especial protección, el consumo de productos, preparados o sustancias o la utilización de técnicas de ingestión o eliminación de productos alimenticios cuyo uso sea susceptible de generar riesgo para la salud de las personas. Las penas previstas para este delito son la de multa de seis a doce meses o prisión de uno a tres años.

Como se puede comprobar, los bienes jurídicos afectados son diferentes. En el primer caso, el del artículo 143 bis, el bien jurídico sería el de la vida humana independiente (homicidio y sus formas); en el caso del 156 ter, se tutela la integridad física (lesiones), y en el artículo 189 bis la protección se encuentra en el ámbito de los delitos contra la libertad e indemnidad sexuales. Para finalizar, la conducta prevista en el artículo 361 bis se dirige al amparo del bien jurídico de la salud pública.

Con esta regulación se va a intentar proteger a las personas menores de edad frente a estos contenidos, pero no hay que olvidar que va a ser complicado, entre otras razones, por la dificultad de persecución y castigo de los delitos tecnológicos.

---

[89] LLORIA GARCÍA, P.; «La LO 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia y la transformación del Código Penal. Algunas consideraciones», *Igualdad.ES*, n.º 6, enero-junio 2022, pp. 293-294. Para esta autora: *«esta técnica de peligro hipotético o presunto hay que enlazarla con la configuración de un bien jurídico colectivo y abstracto, que se puede cifrar en la idea de seguridad».*

[90] BOE. Ley Orgánica 4/2023, de 27 de abril, para la modificación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, en los delitos contra la libertad sexual, la Ley de Enjuiciamiento Criminal y la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2023-10213

Junto a ello, hay que recordar que la gran mayoría de la juventud sigue activamente a personas que crean contenido *online* e *influencers*, especialmente a través de *Instagram* (81,6 %), la red social más popular, seguida de *YouTube* (58,9 %) y *TikTok* (55,6 %)[91].

A petición de la Presidencia española del Consejo de la UE (2º semestre de 2023), el Comité Económico y Social Europeo (CESE) ha emitido un Dictamen sobre *La publicidad a través de influencers y su impacto en los consumidores*[92]*.* En esta consulta, se exponen una serie de conclusiones y recomendaciones de interés. El CESE considera necesario intervenir para garantizar un tratamiento armonizado para las actividades ilegales «específicas» de los creadores de contenido/*influencers* en la UE, residentes o no con obligaciones igualmente específicas para administradores de las plataformas y redes sociales en las que operan. Además, solicita a los administradores de plataformas y redes sociales que sean solidariamente responsables del contenido ilegal publicado por *influencers*, con obligación de denunciar la actividad ilícita, así como de efectuar las acciones necesarias para neutralizar la comunicación *online* objeto de ilicitud.

Igualmente, insta a las plataformas y redes sociales a garantizar la posibilidad técnica de excluir a los usuarios menores de edad de la audiencia de la plataforma y/o redes sociales para todo contenido sensible (alcohol y bebidas energéticas, juegos de azar y apuestas, pornografía, tabaco y derivados, incluidos los cigarrillos electrónicos, cirugía estética, etcétera) que, en todo caso, deberá contener la etiqueta «*prohibido a menores de 18 años»*, obligar a la verificación de edad y permitir el uso del control parental, deberá incluir la mención de «*imágenes retocadas»* cuando estén modificadas o manipuladas y, para producciones creadas con inteligencia artificial, la indicación «*imagen virtual».* Estas cuestiones han sido tenidas en cuenta en el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales.

Como hemos anticipado, las redes sociales influyen en la forma en que los y las adolescentes ven a los demás, tienden a compararse con sus amigos, amigas o seguidores, con un impacto negativo en sus relaciones personales, aumentando la sensación de competencia y envidia que se hace depender del número de «me gusta» recibidos en confrontación con sus iguales.

Los y las adolescentes reciben la influencia de las noticias falsas o información errónea o sesgada, lo que puede afectar a su manera de pensar y de tomar decisiones. Asimismo, el problema de la violencia de género en la juventud es alarmante y las redes sociales tienen un impacto significativo en este asunto[93].

---

[91] El informe *Consumir, crear, jugar. Panorámica del ocio digital de la juventud*, realizado por el Centro Reina Sofía sobre Adolescencia y Juventud de la Fundación FAD Juventud, analiza las prácticas de ocio digital de adolescentes y jóvenes. Para llevar a cabo este estudio, se encuestó a 1200 jóvenes de entre 15 y 29 años residentes en España. En FAD, informe Consumir, crear, jugar. Panorámica del ocio digital de la juventud, 2022. Disponible en: https://www.centroreinasofia.org/publicacion/investigacion_ocio_digital/

[92] UE. Dictamen del Comité Económico y Social Europeo sobre «*La publicidad a través de influencers y su impacto en los consumidores» (Dictamen exploratorio a petición de la Presidencia española*), 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52023AE1658

[93] FEDERACIÓN DE MUJERES JÓVENES. *Informe 'App sin violencia sexual'. Investigación sobre las violencias sexuales que las mujeres sufren en aplicación de citas*, 2022. Disponible en: https://mujeresjovenes.org/recurso/informe-apps-sin-violencia-sexual/

Como hemos dicho, las plataformas en línea pueden amplificar y perpetuar comportamientos abusivos y estereotipos de género, al mismo tiempo que brindan nuevas maneras de ejercer violencia. En la adolescencia, pueden verse influidos por imágenes y mensajes que presentan relaciones desiguales, roles de género rígidos y comportamientos violentos como algo común o aceptable[94].

En este ámbito, se puede constatar como un gran número de chicas adolescentes han experimentado acoso sexual en línea que no proviene de su pareja. Las situaciones más comunes de esta forma de violencia contra las mujeres, en las que una alta proporción de chicas entre 14 y 20 años ha admitido haber vivido al menos una vez, incluyen mostrar imágenes o pedir fotografías sexuales, recibir mensajes sexuales no deseados y solicitudes de cibersexo en línea. Además, un porcentaje significativo de chicas ha mencionado haber sido presionadas para hablar de sexo incluso después de expresar su deseo de detenerse y también han experimentado la difusión de rumores en línea sobre su comportamiento sexual[95].

Como ejemplo de estas situaciones, se puede citar el caso reciente de un grupo de *WhatsApp*, conformado por 199 estudiantes de primero y segundo de Magisterio de la Universidad de La Rioja, donde se emitieron mensajes de contenido machista. En el chat, los chicos adjuntaban fotos de sus nuevas compañeras obtenidas en las redes sociales, para hacer comentarios machistas y vejatorios[96]. Hay que añadir que, todavía hoy en día, en términos de sexualidad, persiste el mensaje de la mujer pasiva y receptiva, lo que hace que aquellas mujeres que tienen personalidad asertiva o iniciativa sexual sigan en ocasiones sintiendo rechazo o crítica.

En definitiva, numerosas redes sociales y aplicaciones muchas veces actúan, según hemos visto, como catalizadores de la violencia hacia las mujeres y las niñas.

2. PORNOGRAFÍA Y MENORES

2.1. *Concepto de pornografía infantil*

La pornografía infantil no es un fenómeno reciente, sino que alude a una realidad criminal compleja que ha venido acentuada por el desarrollo de las TIC, redes sociales e Internet.

---

[94] ONTSI. *Violencia digital de género: una realidad invisible*, 2022. Disponible en: https://www.ontsi.es/es/publicaciones/violencia-digital-de-genero-una-realidad-invisible-2022

[95] INJUVE. *Estudio Violencia de género en la juventud. Las mil caras de la violencia machista en la población jove*n, 2022. Disponible en: https://www.injuve.es/sites/default/files/adjuntos/2022/03/revista-estudios-juventud-125.pdf

[96] Según noticias publicadas en prensa. PÚBLICO.ES., Estudiantes de Magisterio en La Rioja lanzan mensajes machistas hacia sus compañeras: «Hay que partirles las bragas», septiembre 2023. Disponible en: https://www.publico.es/mujer/estudiantes-magisterio-rioja-lanzan-mensajes-machistas-companeras-hay-partirles-bragas.html

El Consejo de Europa, en 1989, define la pornografía infantil como:

> «cualquier material auditivo o visual en el que se emplee a un menor en un contexto sexual»[97].

Con posterioridad, en 2011, la Directiva 2011/93/UE del Parlamento Europeo hace una aproximación a lo que se entiende por pornografía infantil, comprendiendo:

> «La pornografía infantil a menudo incluye imágenes que recogen los abusos sexuales a menores perpetrados por adultos. También puede incluir imágenes de menores que participan en una conducta sexualmente explícita, o de sus órganos sexuales, producidas o utilizadas con fines claramente sexuales y explotadas con o sin el conocimiento del menor. Además, el concepto de pornografía infantil también abarca las imágenes realistas de menores en las cuales el menor participa, o se le representa participando, en una conducta sexualmente explícita, con fines principalmente sexuales».

Según los Convenios de Budapest y de Lanzarote, las conductas constitutivas de pornografía infantil incluyen «*actos reales o simulados*»[98] (entre los que se incluyen los *fakenudes* o desnudos simulados con apariencia real creados a través de la inteligencia artificial) que sean constitutivos de «*relaciones sexuales entre niños o niños y adultos*», independientemente si estos actos son reales o simulados para poder considerarse como material pornográfico. Apuntar que estas conductas son punibles como pornografía infantil, como también recoge el Código Penal. Sin embargo, estas imágenes irreales no se corresponderían con el bien jurídico protegido en el art. 189 de nuestro Código.

Con la reforma de la Ley Orgánica 1/2015, de 30 de marzo, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, se establece una definición legal, derivada de la Directiva 2011/93/UE artículo 2, sobre lo que se considera pornografía infantil o de personas con discapacidad necesitadas de especial protección. En este sentido y, siempre haciendo referencia a representaciones visuales, se dice que entrarán en este concepto:

a) Todo material que represente de manera visual a un menor o una persona con discapacidad participando en una conducta sexualmente explícita, ya sea real o simulada.

b) Toda representación de los órganos sexuales de un menor o persona con discapacidad con fines principalmente sexuales.

c) Todo material que represente de forma visual a una persona que parezca ser un menor participando en una conducta sexualmente explícita, real o simulada, o cualquier representación de los órganos sexuales de una persona que parezca ser un menor, con fines principalmente sexuales, salvo que la persona que parezca ser un menor resulte tener en realidad dieciocho años o más en el momento de obtenerse las imágenes.

---

[97] BOE. *Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015*, 2015. Disponible en: https://www.boe.es/buscar/doc.php?id=FIS-C-2015-00002#:~:text=El%20Consejo%20de%20Europa%20perfil%C3%B3,Recomendaci%C3%B3n%20(91)%2011)

[98] Vid., STS núm. 325/2023, Sala 2ª, de lo Penal, de 10 de mayo, Rec. 10736/2022, que condena al acusado por varios delitos: pornografía infantil, trato degradante hacia menores, descubrimiento y revelación de secretos y falsedad documental. Se le acusó de tomar fotografías y vídeos de menores en situaciones comprometedoras y de modificar digitalmente algunas de estas imágenes para incluir contenido sexual explícito.

d) Imágenes realistas de un menor participando en una conducta sexualmente explícita o imágenes realistas de los órganos sexuales de un menor, con fines principalmente sexuales[99].

Con esta definición, desde un punto de vista meramente descriptivo, se incluye también en el ámbito de aplicación del CP la pornografía virtual, lo que ha llevado a los tribunales a incluir algunos casos de *deepfakes* como de porno infantil, ya que en la propia Directiva europea 2011/93/UE del Parlamento Europeo y del Consejo, se preveía la discrecionalidad de los Estados miembros para regular o no ciertas modalidades de material pornográfico como la pornografía técnica y la pornografía virtual o artificial. Pues bien, nuestro legislador tomó a bien trasladar a la legislación penal la definición de ambas formas de pornografía infantil en su integridad, lo que ha dado lugar a controversias entre la doctrina y la jurisprudencia.

La Fiscalía, continuando la línea jurisprudencial mencionada, adopta una postura restrictiva, estando de acuerdo en penalizar estas conductas como pornografía infantil, aludiendo a la definición que el Diccionario de la Real Academia Española de «realista», conforme al cual significa que «trata de ajustarse a la realidad». Por tanto, la expresión «imágenes realistas» se referirá a aquellas cercanas a la realidad a la que tratan de imitar. Dicho de otro modo, serían imágenes que, no siendo reales, lo parecen, por lo que se podrían incluir aquellas representaciones visuales alteradas de personas reales e incluso aquellas generadas por inteligencia artificial.

La doctrina considera que la ausencia de un menor real sometido a cualquier tipo de conducta sexual o pornográfica hace que sea más que discutible lo correcto de la decisión de incorporar esta conducta a un tipo que aparece ubicado en un título referido a la libertad y/o indemnidad sexual, bienes jurídicos que no se ven realmente afectados.

Se considera que la mera alteración de la voz de un menor o su imagen constituirían una vulneración del derecho a la intimidad o a la propia imagen, lo que supondría que el bien jurídico protegido sería el de la dignidad del menor o el de la propia imagen[100], pues lo que realmente se está castigando es la pura alteración gráfica o auditiva, lo que literalmente interpretado, en palabras de MUÑOZ CONDE, puede llevar a la punición de la utilización de imágenes virtuales sin ninguna base real. Por ello, este mismo autor se cuestiona si no nos encontramos ante un Derecho penal de autor que penaliza la tendencia pederasta como tal, aún sin traducirse en actos que incidan directamente en el menor[101], menoscabando principios tan básicos de nuestro Derecho penal como pueden ser el de intervención mínima, el de exclusión de bienes jurídicos y, por supuesto, el de *ultima ratio*[102].

---

[99] BOE. *Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por Ley Orgánica 1/2015*, 2015. Disponible en: https://www.boe.es/buscar/doc.php?id=FIS-C-2015-00002#:~:text=El%20Consejo%20de%20Europa%20perfil%C3%B3,Recomendaci%C3%B3n%20(91)%2011)

[100] Vid., SAP núm. 298/2007, de 10 julio. En el mismo sentido, CÓRDOBA RODA, J., GARCIA ARÁN, M.; «Comentarios al Código Penal», *Madrid,* Ed. Marcial Pons, 2004, Tomo I, pp. 417-435.

[101] MUÑOZ CONDE, F.*;* «Derecho Penal. Parte Especial», Valencia, Tirant lo Blanch, 2023, pp. 259.

[102] MORENO ACEVEDO, R.; «Los delitos relativos a la captación o utilización con fines exhibicionistas o pornográficos, o para la elaboración de pornografía infantil, art. 189.1 a)». *Revista Electrónica de Ciencia Penal y Criminología*, 2023. Disponible en: http://criminet.ugr.es/recpc/25/recpc25-17.pdf

En los supuestos de pseudopornografía, el peligro para el referido bien jurídico aún se hace más difuso, porque nunca se han utilizado menores para elaborar los materiales. Puede entenderse que, en estos supuestos, se está penando, por medio de un delito de peligro abstracto, la dignidad de la infancia. El peligro no queda concretado o materializado en un menoscabo de la personalidad de los menores, puesto que no han intervenido en las escenas pornográficas.

Ahora bien, la argumentación de penalizar este tipo de pornografía técnica o virtual radica en razones de política criminal, siendo el problema que se plantea el poder distinguir entre imágenes reales e imágenes generadas ficticiamente mediante inteligencia artificial[103]. En aquellos casos en que, siendo la diferencia entre ambas difícil de apreciar, no bastará con la mera asociación de caracteres comunes a cualquier menor, sino que habrá que tener en cuenta rasgos que sean característicos del menor representado para poder aplicar el tipo penal de pornografía infantil, cuando de forma expresa pueda conocerse que en los actos pornográficos representados aparecen menores de edad.

La convicción, o no, muchas veces procederá de la observación directa del tribunal conforme a su criterio valorativo racional, el cual podrá comprobar por la estatura, rostro, falta o no de desarrollo físico sexual (por ejemplo, ausencia de vello púbico), la edad aproximada de los mismos, etcétera[104].

Obviamente, si el menor que aparece en el montaje es producto de un programa informático que no represente o altere gráficamente la imagen de un menor, no cabe incriminación alguna en tanto no existe afectación del objeto tutelable, por cuanto la mencionada representación resulta totalmente ficticia. Por lo tanto, es comprensible entender que la prohibición del referido material fuera una injustificada limitación a la libertad de expresión[105]. Sin embargo, este tipo de pornografía parece que pretende sancionarse en la reforma de 2013 al Código Penal.

Es más, al respecto, cabe añadir que, en el artículo 4.3 de la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor, se establece que «*se considera intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor, cualquier utilización de su imagen o su nombre en los medios de comunicación que pueda implicar menoscabo de su honra o reputación, o que sea contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes legales»*. Así, siendo prevista en el ámbito civil como intromisión ilegítima al derecho al honor, intimidad personal y propia imagen del menor, podía ser sancionada, en las modalidades más graves de ataque, por el art. 197 CP, dedicado a la protección del derecho a la intimidad y a la propia

---

103 MORALES PRATS, F.; «Los ilícitos en la red (II): pornografía infantil y ciberterrorismo», en ROMEO CASABONA, C.M.; «El cibercrimen», Granada, Comares, 2006, pp. 271-297.

104 Vid., SAP de Madrid núm. 489/2009, Sección 3, de 16 de noviembre, Rec. 62/2009, el Tribunal tras el «visionado de las grabaciones correspondientes a las películas y fotografías intervenidas en el domicilio de la DIRECCION000 reveló que su contenido sexual, con relación a los hechos enjuiciados, es siempre relativo a mujeres jóvenes que en la mayoría de los casos presentan indiscutiblemente una edad inferior a los dieciocho años. Así lo revela su apariencia física, complexión y desarrollo y nada permite afirmar que se trate de mujeres mayores de 18 años de aspecto aniñado, real o logrado artificialmente, encontrándonos ante una pseudopornografía».

105 MORALES PRATS, F.; «Pornografía infantil e Internet: la respuesta en el Código Penal español», en MARTÍN-CASALLO LÓPEZ, J.J.; «Problemática jurídica en torno al fenómeno de Internet», Cuadernos de derecho judicial, 2000, n.º 4, pp.175-205.

imagen. Parece que con la vigente redacción del art. 189 del Código Penal el legislador trata de evitar la más mínima fisura en la represión de estas conductas.

2.2. *Tipología penal de la pornografía infantil*

El delito de pornografía infantil se encuentra regulado en el artículo 189 del Código Penal, dentro del capítulo V relativo a la prostitución, explotación sexual y corrupción de menores. Este artículo establece varias modalidades de conducta típica: de una parte, la captación o el uso de menores de edad o personas necesitadas de especial protección para fines exhibicionistas o pornográficos y la elaboración de material pornográfico y, de otra parte, las actividades de producción, venta, distribución, exhibición o cualquier medio de material con contenido de pornografía infantil[106]. Todas las conductas típicas citadas se incluyen con una finalidad sexual[107].

Debido a la naturaleza del tipo penal que nos encontramos analizando, la protección de los menores debe ser, en todo caso, una cuestión prioritaria por la gravedad de las conductas. Al respecto, la Fiscalía determina que, con la pornografía infantil, se daña la dignidad de los niños y niñas, aumenta la reincidencia y la demanda de este tipo de material; dando lugar a nuevos delitos[108]. En el mismo sentido se manifiesta el Tribunal Supremo, indicando que la protección de la indemnidad sexual del menor o incapaz debe ser una protección esencial, ya que el concepto de indemnidad alude a la intangibilidad de la dignidad de la persona y tutela el derecho al desarrollo correcto de la sexualidad[109] con una adecuada formación del menor respecto a su personalidad en materia sexual[110]. En este sentido, la STS núm. 271/2012, Sala 2ª, de lo Penal, de 26 de marzo, Rec. 1605/2012, define la pornografía infantil como «*cualquier material audiovisual que utiliza niños en un contexto sexual».*

La pornografía virtual implica la creación artificial, pero realista, de la imagen de un menor, realizada a través de medios informáticos u otros. La Directiva 2011/93/UE exigía la criminalización de la posesión, producción y distribución de este tipo de pornografía infantil virtual. La modificación del artículo 189.1 d), tras la reforma 1/2015, cumple con lo establecido en la Directiva de 2011, tipificando las conductas relacionadas con los materiales virtuales. En este sentido, se considera como tal, de acuerdo con la definición de la Directiva, las representaciones realistas de un menor participando en actividades explícitamente sexuales o imágenes detalladas de los órganos sexuales de un menor, con un claro propósito sexual. Para evitar interpretaciones erróneas, se debe dar un alcance restrictivo al término «imágenes realistas».

---

106 Vid. STS núm. 795/2009, Sala 2ª, de lo Penal, de 28 de mayo, Rec. 11466/2008, matiza la diferencia entre los apartados a) y b) del artículo 189, reflejando lo siguiente: «*hay que entender se refiere a las conductas del sujeto activo relativas al tráfico o difusión de imágenes pornográficas sin que el mismo haya participado previamente en la elaboración o filmación de las mismas, siendo indiferente la concurrencia o no de ánimo de lucro».*

107 MUÑOZ CONDE, F.*;* «Derecho Penal. Parte Especial», Valencia, Tirant lo Blanch, 2023, pp. 259.

108 BOE. Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015. Disponible en: https://www.boe.es/buscar/doc.php?id=FIS-C-2015-00002

109 Vid. STS núm. 988/2016, Sala 2ª, de lo Penal, de 11 de enero, Rec. 10342/2016.

110 Vid. STS núm. 109/2017, Sala 2ª, de lo Penal, de 22 de febrero, Rec. 10439/2016.

Por lo tanto, no se incluirían dibujos animados, mangas u otras representaciones similares, ya que no se consideran como «imágenes realistas», al no intentar simular la realidad de manera precisa. Así pues, las imágenes generadas por ordenador son sancionables a través del artículo 189 CP, pero deben ser realistas. Sólo serán incluidas dentro del concepto de pornografía infantil aquéllas que se «*aproximen en alto grado a la representación gráfica de un auténtico menor, o de sus órganos sexuales*»[111].

La pornografía técnica consiste en material que muestra a personas pareciendo ser menores en contextos sexuales. La Directiva 2011/93/UE define la pornografía infantil como material que represente a una persona que parezca ser menor participando en conductas sexualmente explícitas, con fines principalmente sexuales. Tras la reforma de 2015, se considera pornografía técnica todo material que presente a una persona aparentando ser menor en contextos sexuales, a menos que la persona realmente sea mayor de edad. La Fiscalía General del Estado interpreta esta disposición considerando el aspecto externo de la persona y el contexto en el que se encuentra, incluyendo texto o audio. El material será considerado penalmente relevante si muestra a personas aparentando ser menores en contextos sexuales, ya sea mediante rasgos aniñados, maquillaje, simulaciones o retoques digitales. Se excluirá la condena cuando el protagonista de la escena pornográfica fuera mayor de 18 años. Si no puede determinarse la edad de la persona representada y el material se expone como relativo a menores de edad, se entenderá como pornografía infantil.

Igualmente, compartir archivos empleando Internet con contenido pornográfico se entiende que entra dentro del tipo penal de distribución, aunque no sea remitido el material, si permite el acceso al mismo por otras personas.

Junto a lo expuesto, el artículo 189 contempla una serie de supuestos agravados que serán castigados con la pena de prisión de cinco a nueve años, cuando concurra alguna de las circunstancias siguientes: cuando se utilice a menores de dieciséis años; se realicen o representen actos violentos o degradantes; cuando se utilice a menores en situación de especial vulnerabilidad; cuando se hubiera puesto en peligro la vida o la salud de la víctima de forma intencional o por imprudencia grave; en los casos de material pornográfico de notoria importancia; cuando el culpable pertenezca a una organización o asociación criminal; cuando el responsable sea ascendiente, tutor, curador, guardador, maestro o cualquier persona encargada, de hecho, de la persona menor o persona con discapacidad o se trate de cualquier persona que conviva con él o de otra persona que haya actuado abusando de su posición de confianza o autoridad, y cuando concurra reincidencia.

Respecto de la agravante de «material pornográfico de notoria importancia», es interesante reflexionar sobre qué se considera «notoria importancia», siendo este un concepto jurídico indeterminado que puede dar lugar a generar inseguridad jurídica.

La Fiscalía General del Estado, en la Circular 2/2015 de 19 de junio ya citada, aboga por aplicar esta agravante teniendo en cuenta la difusión masiva y no el valor económico ni la acumulación del material. En el caso de material virtual o técnico considera su aplicación, siempre que el material hubiera sido objeto de difusión o estuviera dispuesto para la difusión.

---

[111] BOE. Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015. Disponible en: https://www.boe.es/buscar/doc.php?id=FIS-C-2015-00002

Por otro lado, la jurisprudencia, en un primer momento señalaba que habría que estar a la determinación pericial del valor económico de los archivos[112], y por lo tanto, constatando la presencia de una trascendente relevancia económica, la búsqueda de lucro constante y la determinación en el *factum* de dicha dimensión económica. Sin embargo, se abandona esta idea de contenido económico y se busca la fundamentación de la agravante en la mayor intensidad del injusto que representa la afectación del bien jurídico, en aquellos casos en los que la difusión del material pornográfico se ve facilitada por el ingente acopio de archivos susceptibles de ser difundidos. La fijación del ámbito típico que define el precepto agravado de «notoria importancia» lo que aconseja es excluir la aplicación del tipo agravado en aquellos casos en los que no conste acto de difusión.

No serán de aplicación a la pornografía virtual o técnica las agravantes referidas a la utilización de menores de 16 años, el empleo de trato degradante o vejatorio o el peligro para la vida o salud de la víctima. Tampoco las que tienen que ver con las situaciones de parentesco o superioridad o abuso de confianza, ya que cualquier agravación de naturaleza personal en la pornografía técnica o virtual sería imposible atendiendo a la inexistencia de la persona menor, conforme a la postura doctrinal.

2.3. *Modelos de regulación de la pornografía*

Llegados a este punto, es preciso detenerse, por un lado, en la violencia estructural hacía las mujeres existente en la pornografía y, por otro, plantear los modelos su regulación.

---

[112] Para ello, la STS núm. 395/ 2021, Sala 2ª, de lo Penal, de 6 de mayo, Rec. 10258/2020 señala que:
«*De este modo, considerando también las otras agravaciones que modalizan la acción desde la culpabilidad de su autor (circunstancias f), g) y h), puede constatarse que la agravación de notoria importancia viene claramente relacionada (quizás no sólo, pero desde luego fundamentalmente) con la trascendencia o la relevancia cuantitativa del material obtenido. Es evidente que esta demasía es predicable del comportamiento global por el que se ha condenado al recurrente, lo que en principio debería conducir a la desestimación del motivo, pero debe adelantarse que la relevancia cuantitativa del material se desvanecerse respecto de cada uno de los delitos en los que se descomponga el delito continuado. Algo que se abordará con ocasión del recurso interpuesto por el Ministerio Fiscal».*

En el Mismo sentido la STS núm. 494/2023, Sala 2ª, de lo Penal, de 22 de junio, Rec. 3986/21 dice:
«3.3.- Por consiguiente, a raíz de la reforma operada en el año 2010, la actual agravación prevista en el art. 189.2.e) del CP abandonó su significación económica, justificando su aplicación por la mayor intensidad del injusto que representa la afectación del bien jurídico en aquellos casos en los que la difusión del material pornográfico se ve facilitada por el ingente acopio de archivos susceptibles de ser difundidos. Se trata, desde luego, de un concepto normativo –notoria importancia– que impone un proceso de valoración jurisdiccional con el fin de delimitar su ámbito. Y en ese proceso de delimitación ha de quedar fuera cualquier significación económica que, en el texto anteriormente vigente, no hacía sino dificultar la prueba de la concurrencia de la agravación. Carecería de sentido hacer depender el tipo agravado del apartado e) del art. 189.2 de una valoración pericial que ha de esforzarse en la búsqueda de una tasación cuantitativa a un material que, por definición, está fuera del mercado y no es objeto, como regla general, de transacciones onerosas. La fijación del ámbito típico que define el precepto agravado de "notoria importancia" aconseja excluir aquellos casos en los que no conste acto de difusión. La ingente posesión de archivos pornográficos destinados con exclusividad a su visionado por el autor de las descargas no debería ser sancionada con la exasperación de la pena prevista en el art. 189.2.e) del CP».

En primer lugar, reflejar cómo la pornografía en sus representaciones perpetúa constantemente una violencia estructural hacia las mujeres, al objetivarlas y deshumanizarlas en un contexto que prioriza el placer masculino por encima de su bienestar y refuerza la idea de que el valor de las mujeres se encuentra en su apariencia física. Las mujeres son representadas en roles sumisos, donde su consentimiento y sus deseos son ignorados, lo que fortalece una cultura de desigualdad y estereotipos dañinos. En la pornografía se incluyen imágenes de agresiones o humillaciones como excitantes o deseables, influyendo así en la percepción de lo que es aceptable en las relaciones sexuales. Esto provoca que dichos comportamientos abusivos o degradantes sean normalizados de tal forma que cuando se habla de las agresiones sexuales y del sexo, llegando a minimizar las experiencias de las mujeres, ignorar sus deseos y sus límites. Esta circunstancia afecta a la percepción que la sociedad tiene de las mujeres e impacta en la forma en que ellas mismas se ven y se valoran, perpetuando el ciclo de la violencia.

Y, en segundo lugar, en relación con el modo de abordar la normativa en materia de pornografía, se puede mencionar la clasificación que ofrece ARÁNGUEZ SÁNCHEZ, quien apunta a tres modelos legislativos[113]:

1. *Modelo prohibicionista*: predomina en las sociedades tradicionales y está basado el castigo penal a la pornografía, ya que se sustenta en su inconformidad con la moral judeocristiana y sus valores de castidad y sacralidad del matrimonio.
2. *Modelo liberal:* es el modelo imperante en Estados Unidos y en la Unión Europea. Considera que la pornografía es una forma de libertad de expresión, ligada a la esfera privada y al entretenimiento, al arte y a la información. Las leyes liberales sostienen que las páginas pornográficas son simplemente plataformas que alojan contenido y no tienen responsabilidad legal por la pornografía que ofrecen. Sólo están obligadas a contar con un mecanismo interno para que los usuarios reporten contenido ilegal. Los menores pueden acceder a la pornografía sin restricciones, ya que no se requiere verificar su edad; aunque sí se advierte de que se trata de contenido pornográfico.
3. *Modelo abolicionista:* sistema apoyado por países como Reino Unido y Australia. Se centra en proteger los derechos de las mujeres y de los niños y de las niñas. Los dos estados implementaron un sistema administrativo para buscar y clasificar contenido pornográfico ilegal. La finalidad es prevenir que las personas menores accedan a la pornografía a través de sistemas de verificación de edad y de filtros en línea. Estos países amplían la definición de pornografía ilegal para incluir en su ámbito de prohibición prácticas violentas o degradantes hacia las mujeres. Además, el modelo abolicionista penaliza el consumo de pornografía ilegal, imponiendo sanciones a los usuarios. También incluye medidas educativas para desalentar el consumo de este tipo de contenidos.

---

[113] ARÁNGUEZ SÁNCHEZ, T.; «Tres modelos legislativos de la pornografía». *Revista Internacional de Estudios Feministas,* v 6, n.º 1, 2021, pp. 165-189.

Por último, debemos hacer una reflexión sobre los efectos nocivos del consumo de pornografía en personas menores de edad. Concretamente, La Sociedad Española de Medicina de la Adolescencia refiere que: «*los adolescentes se encuentran en un período evolutivo crítico para el desarrollo de una sexualidad sana, por los diversos cambios biológicos, afectivos, psicológicos y sociales propios de esta etapa, parece que son más susceptibles ante la exposición a este tipo de contenidos*».

La exposición temprana a la pornografía acarrea una serie de riesgos y daños significativos para el desarrollo emocional y psicológico. La AEPD, la ONG «Dale una vuelta» y la Fundación del Colegio Oficial de Psicología de Madrid han recogido en un decálogo[114] 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, en este decálogo se advierte que el consumo ocasional de pornografía puede conducir a un comportamiento adictivo en menores de edad y adolescentes. Este patrón se manifiesta a través de una mayor tolerancia, dependencia, pérdida de control, síntomas de abstinencia, dificultades para gestionar las emociones con la pornografía, así como conflictos en diversas áreas de la vida y una creciente necesidad de consumir este tipo de contenido. Esto, a su vez, puede promover el aislamiento social y la disminución de actividades interpersonales en la adolescencia.

Además, el acceso de los menores de edad a la pornografía como medio de aprendizaje está vinculado a una falta de información sobre sexualidad y a una proliferación de estereotipos de género, lo que contribuye a la normalización del sexismo y a la reproducción de actos, creencias y actitudes violentas en el ámbito sexual, incluyendo comportamientos de abuso físico y verbal en las relaciones de pareja. Al mismo tiempo, supone un aumento de las conductas sexuales de riesgo –entre otras– uso irresponsable del preservativo, practicar relaciones sexuales bajo los efectos de sustancias o el consumo de prostitución– vinculándose de igual modo con la promiscuidad sexual, infidelidad e iniciación temprana al sexo.

2.4. *Líneas de protección*

Ante esta situación, frente a los diversos riesgos se han ido perfilando líneas encaminadas a la protección de los y las menores.

En el ámbito europeo, en el año 2020 se inicia la primera estrategia para la lucha de los peligros que pueden sufrir los y las menores en entornos digitales con la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, creando la *Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores*, de 24 de julio.

---

[114] AEPD, DALE LA VUELTA, FUNDACIÓN COLEGIO OFICIAL DE LA PSICOLOGÍA DE MADRID. *El impacto de la pornografía en menores*. Disponible en: https://www.infocop.es/wp-content/uploads/2024/10/el-impacto-de-la-pornografia-en-menores.pdf

Precisamente, esta estrategia pretende la creación de una respuesta firme ante el abuso y agresiones sexuales de menores, fomentando la prevención a través de la implantación de cursos, campañas, materiales didácticos y un código de buenas prácticas e investigación de los casos sospechosos. Y estableciendo la asistencia para las víctimas de abuso, que se hace realmente necesaria para reducir las consecuencias psicológicas de los procesos de victimización tras el impacto del hecho traumático.

Por otro lado, la apuesta europea por la cooperación es esencial. En este sentido, los ministros de Justicia y Asuntos de Interior de los Estados miembros de la UE encargaron a Europol la creación de un laboratorio de innovación para apoyar a los y las profesionales de la policía en el ámbito de la innovación. Por ello, Europol crea el «*Laboratorio para la Innovación*» para la dotación de herramientas innovadoras y más eficaces para la protección de la ciudadanía, evitando la duplicación de esfuerzos entre las Fuerzas y Cuerpos de Seguridad. Especialmente, herramientas que permitan la lucha contra el abuso sexual a menores en entornos digitales.

Asimismo, anteriormente, en 2012, la Comisión Europea en la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones desarrolló la primera Estrategia europea para mejorar la experiencia de los niños en Internet (*BIK*). Este marco, referente mundial, influye en las políticas desarrolladas de la Unión Europea. La estrategia *BIK* desempeña un papel crucial en la protección y en la formación de los y las menores en el ámbito digital europeo, nacional e internacional. Creó una red de Centros de Seguridad en Internet, cofinanciada por la UE y el portal *betterinternetforkids.eu,* donde se centraliza información sobre la seguridad en línea para niños y niñas. Estos centros realizan actividades de concienciación adaptadas a cada contexto local, brindan materiales sobre seguridad infantil en línea en los Estados miembros, ofrecen ayuda a través de líneas telefónicas de asistencia y apoyan la eliminación de pornografía infantil en línea a través de *INHOPE*[115], presente en cuarenta y seis países. Además, colaboran con una red de embajadores y paneles de jóvenes que aconsejan a los responsables políticos y profesionales sobre la comunicación adaptada a los niños y las niñas.

Igualmente, la estrategia *BIK* ha tenido influencia en el marco jurídico de la UE, que ha evolucionado significativamente para garantizar una mayor seguridad de las personas menores en línea. En este sentido, habría que mencionar: la Directiva UE 2018/1808, que obliga a las plataformas de intercambio de vídeos a proteger a los y las menores de contenido perjudicial; el Reglamento General de Protección de Datos, que establece que su datos personales requieran de una protección especial, y que el consentimiento de los progenitores es necesario hasta cierta edad, entre los 13 y los 16 años, en función del Estado miembro; y la Ley de Servicios Digitales, que obligará a las plataformas en línea a tener en cuenta los derechos de los usuarios menores de edad al diseñar sus sistemas, asegurando que estos puedan comprender fácilmente los términos del servicio que utilizan.

Recientemente, en mayo de 2022, la Comisión Europea introduce mejoras a la primera estrategia *BIK*, con la publicación de la Comunicación sobre *Una década digital para los niños y los jóvenes:*

---

115 INHOPE. Red Mundial de 54 líneas de emergencia, frente a lucha contra el abuso sexual a menores *online*. Disponible en: https://www.inhope.org/EN

la nueva estrategia europea para un Internet mejor para los niños (BIK+)[116], en la que se consulta ampliamente a menores, padres, profesores, Estados miembros, la industria de las TIC, los medios de comunicación, la sociedad civil, el mundo académico y organizaciones internacionales. El objetivo de la estrategia *BIK+* es complementar y respaldar la implementación de medidas existentes para proteger a las personas menores de edad en el entorno digital, fomentar sus habilidades y capacitarlos para disfrutar de Internet de manera segura, tras los peligros advertidos, que va en la misma dirección que las Conclusiones del Consejo sobre la alfabetización mediática 2020/C 193/06[117] y la Recomendación del Consejo por la que se establece una Garantía Infantil Europea[118].

Por ello, los tres pilares de la *BIK+* están enfocados en:

1. Creación de experiencias digitales en Internet que sean realmente seguras para los derechos de los niños y las niñas y mejorar su bienestar en línea a través de un entorno digital seguro.
2. Capacitación digital en personas menores de edad para dotarles de las herramientas para que puedan tomar decisiones sensatas y expresarse en el entorno virtual de manera segura.
3. Participación activa de los niños y niñas, respetándolos y teniendo en cuenta sus opiniones para fomentar experiencias digitales innovadoras, creativas y seguras[119].

En definitiva, las líneas de actuación están centradas en la protección de la infancia y adolescencia garantizando un entorno seguro en Internet y desarrollando los múltiples mecanismos de prevención, formación y capacitación digital.

2.5. *Acceso de las personas menores a los contenidos para adultos*

Durante la minoría de edad, se está en constante formación y en plena etapa madurativa. Es un momento fundamental para la adquisición de valores y principios y para la formación de la personalidad, que requiere de una protección adecuada y rigurosa. Por ello, resulta esencial la evaluación de los peligros y amenazas que pueden ser dañinos en ese proceso. Esto nos conduce a considerar que el acceso de los y las menores a la pornografía *online* es un tema preocupante y que ha aumentado con la popularización de Internet y dispositivos móviles.

---

116 UE. Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Una década digital para los niños y los jóvenes: la nueva estrategia europea para un internet mejor para los niños (BIK+)*, 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik

117 UE. DOUE. *Conclusiones del Consejo sobre la alfabetización mediática en un mundo en constante transformación*, 2020. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XG0609(04)

118 UE. *RECOMENDACIÓN (UE) 2021/1004 del Consejo de 14 de junio de 2021 por la que se establece una Garantía Infantil Europea*. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2021-80844

119 UE. Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Una década digital para los niños y los jóvenes: la nueva estrategia europea para un internet mejor para los niños (BIK+)*, 2022. Disponible en: https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik

A diferencia de la pornografía tradicional, que solía estar limitada a revistas, películas o canales de televisión para adultos, la pornografía *online* está disponible de forma fácil y gratuita, sin control sobre la edad de la persona que accede a dichos contenidos, lo que posibilita que los y las menores puedan tomar contacto con ella de manera inadvertida.

Las diferencias principales entre la pornografía *online* y la tradicional incluyen la asequibilidad, inmediatez, anonimato y la accesibilidad. En Internet, los y las menores pueden acceder a contenidos pornográficos con sólo unos pocos *clics*, mientras que en la pornografía tradicional se requería el acceso a material físico o a canales específicos, existiendo una mayor dificultad de acercamiento, incluso, en muchos casos, quedaba restringido e identificado como contenido para adultos. En ocasiones, esta pornografía no es buscada por los y las menores, sino que la propia configuración de las páginas de manera segmentada les dirige a estos contenidos para adultos. Esta técnica se realiza de manera intencionada y buscada por los posibles pederastas o captadores de menores.

Por otra parte, hay que recalcar que la pornografía *online* suele ser más explícita y violenta que la tradicional, generando un impacto negativo en el desarrollo emocional y psicológico en las personas menores, y ello porque se caracterizada por ser un contenido audiovisual, de alta calidad y diverso, que incluye representaciones explícitas de actividad sexual.

Según el Informe sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica[120]:

> «*La sobreexposición a la pornografía, que contribuye a los estereotipos de género y suele ser el único punto de referencia de los jóvenes para las relaciones sexuales, especialmente en ausencia de acceso a una educación integral sobre sexualidad y relaciones, conduce a una imagen distorsionada y violenta de la sexualidad. Por tanto, los Estados miembros deberían tener en cuenta el impacto de la pornografía en los jóvenes y el riesgo de que reproduzcan comportamientos violentos*» (enmienda 79 al considerando [59]).

Ciertamente, cada vez se accede al contenido pornográfico a edades más tempranas, alrededor de los 8 años, a través de los primeros dispositivos electrónicos, principalmente los móviles[121]. Sin embargo, a nivel cerebral, los niños y las niñas no están preparados para procesar contenidos de impacto violento. La falta de educación sexual y el tabú que rodea a la sexualidad hacen que el porno se convierta en una fuente de aprendizaje privilegiada para la juventud, normalizando la violencia y la cosificación de los cuerpos, especialmente el de las mujeres.

De acuerdo con las recientes investigaciones publicadas en España, el acceso de las personas menores a la pornografía en línea es predominante. El estudio de *Save The Children,* publicado en 2020, *Informe (Des)información sexual: pornografía y adolescencia,* revela que el 68,2 % de los adolescentes

---

120 UE. *Informe sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la lucha contra la violencia contra las mujeres y la violencia doméstica, 2023.* Disponible en: https://www.europarl.europa.eu/doceo/document/A-9-2023-0234_EN.html

121 BALLESTER BRAGE, L., ORTE SOCÍAS, C., y POZO GORDALIZA, R.; «Estudio de la nueva pornografía y relación sexual en jóvenes», *Revista andaluza de Ciencias Sociales,* 2014, n.º 13, pp. 165-178.

consumen contenido pornográfico frecuentemente, al menos una vez al mes. Por su parte, el *Estudio sobre pornografía en las Islas Baleares, acceso e impacto en la adolescencia*[122], publicado en 2022, concluye de forma alarmante que el 93,3 % de los adolescentes antes de los 14 años comienzan a ver pornografía; el 76,25 % consumen pornografía *hardcore* o explícita, y el 90,5 % de la juventud de entre 13 y 18 años admiten haber visto pornografía en los últimos años. Asimismo, este estudio muestra cómo es especialmente relevante la reducción de la diferencia por sexo en la adolescencia en cuanto al acceso a la pornografía: el 91,7 % hombres y el 89,3 % de las mujeres han mirado pornografía en los últimos años.

A este respecto, es importante tener en cuenta lo que afirma la sexóloga GONZÁLEZ ESTEBAN: *«basarse en comportamientos sexuales observados en la pornografía puede conducir a la frustración ya que producen "expectativas irreales" y dificultan la capacidad para imaginar y desarrollar fantasías mentalmente, necesitando la estimulación y visual como única respuesta de excitación»*[123]. En este escenario, resulta conveniente resaltar que la pornografía en línea está teniendo un impacto significativo en la educación sexual y la formación de la identidad de los y las menores y la juventud. Cada vez más, recurren a ella como fuente principal de información sobre sexualidad, lo que puede influir en sus conocimientos y actitudes y en la perpetuación de estereotipos de género basados en el sometimiento y subordinación de la mujer. El fácil acceso a este tipo de contenido en Internet está impidiendo el desarrollo de una sexualidad saludable en la adolescencia y la infancia, promoviendo prácticas de riesgo, agresivas y denigratorias hacia las y los menores de edad y las mujeres y pudiendo limitar la capacidad de establecer relaciones fundamentadas en el respeto mutuo, el consentimiento y el placer compartido.

Además, se puede observar una pérdida de pudor y privacidad, junto con una banalización de la sexualidad, al normalizar el contenido sexual explícito y duro. Las redes sociales también pueden convertirse en lugares donde los y las menores son reclutados para la producción de material pornográfico.

Junto a ello, hay que traer a colación que el consumo de pornografía se ha relacionado con un aumento en los delitos sexuales cometidos por menores. Igualmente, una tendencia preocupante es la grabación y difusión de vídeos de contenido sexual en redes sociales, donde los menores conceden mayor importancia a la obtención de protagonismo y a que se hable de ellos frente a la consideración del posible delito que se está cometiendo. Es necesario iniciar un debate sobre este tema para concienciar sobre sus riesgos y consecuencias.

En cuanto a los retos a los que nos enfrentamos, debemos partir de la realidad de que cada vez más los niños y las niñas son usuarios de las tecnologías digitales, ya que la denominada abstinencia

---

122 IBDONA-UIB. *Estudi sobre pornografia a les Illes Balears: Accés i impacte sobre l'adolescència, dret internacional i nacional aplicable i solucions tecnològiques de control i bloqueig.* Disponible en: https://www.caib.es/pidip2front/adjunto?codi=2952149&locale=es

123 Heraldo.es *«¿Cómo influye la pornografía en los jóvenes?» Heraldo.es. 5 de abril de 2018.* Disponible en: https://www.heraldo.es/noticias/aragon/2018/04/05/como-influye-pornografia-entre-los-jovenes-1233295-300.html

digital no es aceptable en un entorno en el que todo está digitalizado. Concretamente, según datos del INE publicados para el año 2023, el 9,7 % de menores manejan Internet y un 70,6 % usan móvil, 1,1 puntos más que en 2022[124]. Al mismo tiempo, los riesgos son realmente altos y tienen efectos nocivos en su salud y en la vulneración de sus derechos. Todo ello obliga a pensar que es necesaria la implementación de mejoras en los sistemas de verificación de la edad para evitar su acceso a plataformas, redes sociales y contenido no adecuado para su edad, ya que el contenido de imágenes de pornografía e incluso de agresiones sexuales a menores (o a adultos) sigue presente en Internet; se hace también necesario fomentar el acompañamiento por parte de las familias.

Por lo demás, resulta ineludible establecer una protección específica de los datos de menores almacenados en Internet e instaurar mejoras en la alfabetización mediática, incidiendo en una educación que integre una seguridad en Internet que pueda servir como mecanismo de prevención y de lucha contra los peligros a los que puedan enfrentarse los menores de forma *online*.

2.5.1. Medidas de control de acceso de menores a la pornografía en línea en España

Las medidas de control de acceso de menores a la pornografía en línea en nuestro país están encaminadas al establecimiento de un entorno digital seguro para las personas menores.

España, junto a otros ocho países europeos, se ha adherido al *Laboratorio para la protección online de los menores frente a contenidos pornográficos,* creado por Francia en 2022. Este Laboratorio tiene como finalidad investigar, promocionar, desarrollar y examinar soluciones que mejoren la seguridad de los y las menores en línea. Su objetivo es promover el intercambio de información, conocimientos, experiencias y buenas prácticas, así como fomentar la investigación para abordar de manera efectiva los temas que impactan a los menores en el entorno virtual. Singularmente, pone el foco en garantizar la verificación de edad para prevenir la exposición temprana de los y las menores a contenidos pornográficos. Además, señala que 1 de cada 3 niños en el mundo ha estado expuesto a contenidos pornográficos antes de los 12 años, y un tercio reconoce haber sido destinatarios de acoso cibernético[125].

A primeros de 2024, según las noticias publicadas en diferentes medios de comunicación, el Ministerio de la Presidencia, Justicia y Relaciones con las Cortes ha llevado un informe al Consejo de Ministros con una hoja de ruta para controlar y frenar el acceso de los menores a la pornografía en Internet. Este documento, titulado *Informe sobre protección integral de menores frente al acceso a la pornografía en internet*, es un sistema de verificación de la edad que ha sido probado con los principales navegadores y cuyo objetivo principal es proteger a los menores del acceso a la pornografía. Pone de manifiesto el grave impacto en su bienestar y desarrollo emocional, afectivo y sexual. A raíz de este informe, el Gobierno, entre sus objetivos, pretende hacer efectivo un marco legal que prohíba el acceso de

---

[124] INE. Datos estadísticos 2022. Disponibles en: https://www.ine.es/prensa/ec_am_2022.pdf

[125] España impulsa con otros ocho países el refuerzo de la protección de los menores en Internet frente a los contenidos pornográficos, *Moncloa actualidad,* 2023. Disponible en: https://www.lamoncloa.gob.es/servicios-deprensa/notasprensa/asuntos-economicos/Paginas/2023/101123-proteccion-menores-internet.aspx

menores a contenidos pornográficos; promocionar el uso responsable de Internet entre las personas menores de edad, y garantizar su protección frente a las consecuencias del acceso a contenidos inapropiados para su edad. El ejecutivo impulsará una ley de protección de los menores en Internet, que ya se ha materializado en el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en entornos digitales.

Primeramente, deben instaurarse mecanismos adecuados de control de verificación de edad. Actualmente, con carácter general, la comprobación se basa en una autodeclaración de edad o facilitar credenciales al proveedor de contenidos.

Debemos recordar que la Ley 13/2022, de 7 de julio, General de Comunicación Audiovisual, en su artículo 89 e), regula la obligación para los proveedores de contenido de implementar y gestionar sistemas de verificación de edad con el objeto de proteger a los y las menores de contenidos que puedan lesionar su desarrollo físico, mental o moral. En cualquier caso, de aquellos más perniciosos, como la violencia gratuita o la pornografía o autolesión.

En este apartado, es importante subrayar el trabajo de la Agencia Española de Protección de Datos (AEPD) en cuanto a la problemática del acceso de menores a contenido de adultos. En 2019, en la AEPD se constituía un grupo de trabajo sobre menores y salud digital para analizar y hacer propuestas que supongan una mejor protección de las personas menores en el ámbito digital, en el que los servicios que se prestan y los contenidos que se ofrecen a través de redes sociales y servicios equivalentes requieren del tratamiento de datos personales para su operatividad, concluyendo con la presentación de la Estrategia y Líneas de Actuación respecto de Menores, Salud Digital y Privacidad, de 29 de enero de 2024[126].

Entre las distintas iniciativas del grupo de trabajo destacan las siguientes: el Portal *Aseguratic*, que contiene el más amplio repositorio de materiales, recursos y herramientas, catalogadas y ordenadas por materia, edades, fuente y destinatarios (docentes, familias y alumnado), disponible en la web del Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF), en materia de salud digital, impulsando la colaboración y elaboración de herramientas para prevenir y detectar usos inadecuados o adictivos a las TIC, como el Plan Digital Familiar de la Asociación Española de Pediatría. En este sentido, cabe destacar muy especialmente el Decálogo con los criterios y requisitos que han de reunir los sistemas de verificación de la edad en el acceso a contenidos *online* para adultos, de forma que sean eficaces y respetuosos con el marco de protección de datos y privacidad.

Concretamente, con respecto al sistema de verificación de la edad, que busca salvaguardar a los niños y las niñas de material pornográfico o destinado a adultos, se propone un sistema de doble ciego o doble verificación, constituyéndose como un método más garantista con respecto a los países de nuestro entorno, con la finalidad de que este sistema sea el que se instaure en toda la Unión Europea, ya desarrollado en países como Francia o Reino Unido, colaborando en particular con la Comisión Nacional de los Mercados y la Competencia (CNMC), la Fábrica Nacional de Moneda y Timbre (FNMT), el Ministerio del Interior y el Ministerio de Transformación Digital.

---

[126] AEPD. *Protección de datos y prevención de delitos*. Disponible en: https://www.aepd.es/documento/guia-proteccion-datos-y-prevencion-de-delitos.pdf

Es un sistema que pretende garantizar la imposibilidad de localización o seguimiento de menores (trata de impedir identificar entre las personas usuarias de Internet a aquellas que son menores), el anonimato de la persona identificada de cara a los proveedores y terceras entidades, impidiendo o dificultando la realización de perfiles y evitar la vinculación entre la persona y los distintos servicios. Con ello se trata de garantizar el derecho a la intimidad de las personas adultas, que no deben estar controladas por ninguna institución o entidad. Nadie debe conocer quién accede y quién no a contenidos pornográficos o de otra naturaleza, por lo que la identidad de las personas sólo deberá desvelarse en relación con la posible comisión de delitos y con la correspondiente autorización judicial.

También, se completará con el etiquetado inteligente para la identificación y detección de contenido potencialmente perjudicial. Por ello, la AEPD ha realizado una propuesta para llevar a cabo un sistema de etiquetado. Según indica la propia Agencia, la técnica de marcado es graduable, y se puede adaptar a diferentes culturas y religiones y se basa en la autoevaluación (el etiquetado lo realizan los propios proveedores), que podría ser controlada o matizada por diferentes comités y comisiones formadas por autoridades, la industria, asociaciones de padres, etc.

Igualmente, en cuanto a la protección de víctimas de difusión de contenido sexual o violento, especialmente si se trata de menores de edad o víctimas por razón de género, la AEPD dispone de una herramienta fundamental, que es el Canal prioritario[127]. A través de este sistema, se puede solicitar la retirada inmediata de una publicación en Internet de fotografías, vídeos o audios de contenido sexual o violento cuya difusión ilícita pone en grave riesgo los derechos y libertades o la salud física y/o mental de las personas afectadas.

En mayo de 2019, la AEPD adopta el Marco de Actuación de Responsabilidad Social para el periodo 2019-2024[128], en consonancia con los Objetivos de Desarrollo Sostenible de Naciones Unidas. Este Marco de Actuación de Responsabilidad Social se estructura y se presenta claramente en planes anuales consecutivos, donde la AEPD detalla las acciones de responsabilidad social que se llevarán a cabo durante los cinco años que comprende el Marco de Actuación. En su último Plan[129] (correspondiente a 2024), destacan dos áreas de trabajo: una centrada en la protección de los menores en el mundo digital y la otra en la prevención de la violencia de género y la promoción de la igualdad. Entre otras, las medidas más destacables en relación con las personas menores son las siguientes: impulsar y promover en el entorno nacional e internacional los criterios de verificación de la edad, colaborar con las instituciones competentes en el etiquetado de contenidos *online*, publicidad, *cookies* y perfilado de menores y analizar los patrones adictivos. Igualmente, con respecto a la igualdad de género y a las acciones para combatir la violencia de género en Internet, destacan las campañas de concienciación sobre violencia digital contra las mujeres, el impulso de protocolos de actuación y alianzas con

---

127 AEPD. Canal prioritario de retirada de contenidos sensibles. Disponible en: https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/nuevaReclamacion.jsf?QID=Q600&ce=0

128 AEPD. *Marco de Actuación de Responsabilidad Social. AGENDA 2030. (2019-2024).* Disponible en: https://www.aepd.es/documento/marco-actuacion-responsabilidad-social-aepd.pdf

129 AEPD. *Plan Anual 2024 de Responsabilidad Social.* Disponible en: https://www.aepd.es/documento/plan-acciones-rsc-aepd-2024.pdf

organismos y entidades que luchan contra la violencia de género, y reforzar la difusión y promoción del Canal Prioritario a los efectos previstos en la Ley Orgánica de garantía integral de la libertad sexual.

En resumen, todas las medidas centradas en la protección de la exposición de las personas menores al acceso en línea a contenido pornográfico son valoradas positivamente y fundamentales para generar un entorno digital seguro.

2.5.2. Medidas de prevención, formación y concienciación

Para la protección de menores en línea es fundamental la implementación y desarrollo de medidas de prevención, formación y concienciación tanto de las personas menores como de la ciudadanía en su conjunto. Especialmente, en materia de educación afectivo sexual para otorgar herramientas que permitan la comprensión y el manejo de sus emociones, sus sentimientos y sus relaciones interpersonales de manera saludable. Sería clave la inclusión de este tipo de educación en el currículo escolar, ya que las personas menores de edad pasan gran parte de su tiempo en este entorno y es necesario que cuenten con información adecuada y confiable sobre temas relacionados con la sexualidad. El artículo 9 de 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, establece que las administraciones educativas deben garantizar la formación en salud sexual y reproductiva en el sistema educativo, como parte integral del desarrollo personal, la formación en valores y la dignidad de la persona. Además, esta norma menciona la importancia de adoptar un enfoque interseccional en esta formación, que promueva una visión de la sexualidad en términos de igualdad, corresponsabilidad y diversidad, teniendo en cuenta aspectos como el placer, el deseo, la libertad y el respeto.

Destaca la trascendencia de prestar especial atención a la prevención de la violencia de género y la violencia sexual, con el objetivo de fomentar relaciones sanas y respetuosas entre individuos en el ámbito de la sexualidad. En su artículo 10 bis establece que las administraciones educativas deben incluir, dentro de sus competencias y de acuerdo con lo establecido en la Ley Orgánica 3/2020 de Educación[130] y las disposiciones que la desarrollan, la educación afectivo-sexual, la igualdad de género y la educación en derechos humanos en los currículos de las diferentes etapas educativas.

Todas estas medidas tienen como objetivo garantizar la libertad sexual y prevenir las violencias sexuales, incluyendo aquellas que puedan ocurrir en el ámbito digital. Asimismo, se indica que también deben ser incluidas en las ofertas formativas de Formación Profesional establecidas en la Ley Orgánica[131] que la regula. De esta manera, se busca incorporar la prevención de las violencias sexuales en todos los ámbitos educativos, incluyendo la Formación Profesional, y prevenir situaciones de vulnerabilidad en el entorno digital.

---

[130] BOE. Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2020-17264

[131] BOE. Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2022-5139

Por otro lado, las familias tienen un papel primordial en la educación afectivo sexual de sus hijos e hijas, ya que son los primeros referentes en esta materia y pueden brindarles un espacio seguro para abordar estos temas de manera natural y libre de prejuicios.

Como se ha mencionado previamente, es fundamental que tanto las instituciones educativas como las familias se involucren en la educación afectivo sexual de las personas menores de edad, incluyendo la reflexión crítica sobre los contenidos pornográficos, así como la importancia del consentimiento, la comunicación y el respeto en las relaciones sexuales, en una educación orientada a presentar modelos y referentes que demuestren afecto de manera respetuosa, que permitan reconocer los riesgos y oportunidades e identificar las relaciones de poder y rechazarlas, dotándoles de las herramientas necesarias para que puedan tomar decisiones informadas y saludables. Indudablemente, reforzar la autoestima y el autoconocimiento promoverá su autonomía y seguridad personal, fomentando la conversación natural sobre sexualidad que evite tabúes y desmitifique creencias erróneas.

De la misma forma, se requiere el compromiso de las familias y tutores en la instauración de medidas para un uso adecuado y responsable de los dispositivos y evitar que las personas menores de edad accedan a este tipo de contenido pornográfico, o que lo hagan sin acompañamiento según su edad. Para ello, es esencial la adopción de mecanismos de control parental entre los que destacan, entre otros: controlar por edad la cantidad máxima de tiempo que deben pasar en dispositivos electrónicos, instalación de filtros de contenido, restricciones de navegación en las descargas y aplicaciones, monitorear y limitar el acceso a ciertos sitios, activación de un código pin para abrir ciertas funciones, supervisar y gestionar sus cuentas e inhabilitación de ajustes de localización, establecer reglas claras sobre el uso de dispositivos electrónicos y educar sobre los riesgos asociados a la pornografía y otros contenidos violentos, conforme aconseja el artículo 84 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales.

A principios de 2024, la Comisión Europea ha adoptado una *Propuesta de Directiva relativa a la lucha contra los abusos sexuales y la explotación sexual a los menores y el material de abuso sexual de menores y por la que se sustituye la Decisión Marco 2004/68/JAI del Consejo,* para actualizar las normas de Derecho penal sobre abuso sexual de menores y explotación sexual. Estas normas revisadas amplían las definiciones de los delitos e introducen penas más altas y requisitos más concretos en materia de prevención y asistencia a las víctimas. Del mismo modo, complementan la Propuesta de Reglamento por la que se establecen normas para prevenir y combatir el abuso sexual a los menores, presentada por la Comisión en 2022, que establece la obligación de que las empresas de Internet detecten, denuncien y eliminen el material de abuso sexual a menores en sus servicios.

La Propuesta de Directiva establece un paquete normativo para prevenir y combatir el abuso sexual de los menores en el entorno digital y aboga por intensificar la prevención; aumentar la inversión en concienciación, especialmente sobre los riesgos en línea, a fin de velar para que Internet sea más seguro y mejor para las personas menores de edad. Por otra parte, en relación con los proveedores de servicios y plataformas de Internet, la Propuesta de Directiva tiene como fines hacer obligatoria la detección, notificación y retirada de material de abuso sexual infantil y centrarse en mejorar los mecanismos de prevención a través de la formación especializada del personal empleado en estos

servicios, puesto que dichos prestadores frecuentemente son los únicos que están en condiciones de prevenir y combatir tales abusos.

2.6. *Impunidad e invisibilidad del agresor*

Las TIC son herramientas que permiten el anonimato, lo que supone tener la capacidad de ocultar fácilmente la identidad real de un usuario en línea utilizando un pseudónimo o nombre falso, perfiles irreales, avatares, dibujos, fotografías; incluso posibilitar el proceso de alta con diferente sexo o edad. Esto permite a las personas intervenir en las redes sociales y expresar sus opiniones o interactuar con otros usuarios de la red sin revelar su identidad personal. Hay que tener en cuenta lo recogido en la Carta de Derechos Digitales española[132] sobre el derecho a pseudoanonimato:

> «1. De acuerdo con las posibilidades técnicas disponibles y la legislación vigente, se permitirá el acceso a los entornos digitales en condiciones de pseudonimidad, siempre y cuando no sea necesaria la identificación personal para el desarrollo de las tareas propias de dicho entorno.
>
> 2. El diseño de la pseudonimidad a la que se refiere el número anterior asegurará la posibilidad de reidentificar a las personas previa resolución judicial en los casos y con las garantías previstas por el ordenamiento jurídico».

En cuanto a este al anonimato va a ser difícil su limitación, ya que, conforme a la Carta, surge como un derecho en la red.

Este anonimato en las redes sociales aporta ciertas ventajas a las personas internautas, pues facilita el ejercicio de derechos como la libertad de expresión, el sentirse más cómodas compartiendo opiniones o ideas que pueden considerarse controvertidas sin el temor a sufrir represalias o estigmatización, etcétera. Esta falta de determinación de la identidad facilita la protección de la privacidad, evitando que se divulguen detalles personales o se lleven a cabo ataques directos hacia su persona y favorece la participación en foros de comunidades específicas con las que compartir experiencias o intereses comunes sin descubrir su identidad.

Sin embargo, también existen desventajas asociadas a la falta de identificación, como son el posibilitar comportamientos negativos y/o delictivos, tales como el ciberacoso, exponer discursos de odio o llevar a cabo la difusión de información falsa. El acceso a Internet desde conexiones gratuitas *Wifi* en puntos de acceso público, el empleo de aplicaciones que permiten el acceso a la red ocultando la información de identificación del ordenador de origen o el uso de servidores *proxy*, intermediarios entre dos ordenadores para ocultar la dirección IP, contribuyen al anonimato de los delincuentes y a la sensación de impunidad que conduce a que las acciones sean más lesivas y reiteradas. Cada vez en mayor medida, los delincuentes acceden a la transmisión de vídeos de cámaras *web* para ver a las víctimas en tiempo real sin producir o almacenar imágenes o vídeos que luego podrían ser descubiertos

---

[132] ESPAÑA. *Carta de Derechos Digitales española. Plan de Recuperación, Transformación y Resilencia,* 2021. Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

por la policía. El acosador, desde el engaño e impunidad que aporta ese anonimato, realiza la conducta abusiva, teniendo la sensación de dominio sobre la víctima y de imbatibilidad frente a ella.

Es común que en el campo de los videojuegos *online* sean las mujeres quienes oculten su identidad, debido a la percepción que tienen de haber sufrido acoso sexual en mayor proporción, principalmente en los grupos de edad de 15 a 19 años y de 25 a 29 años[133].

A pesar de que la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales prohíbe a los menores de 14 años abrir perfiles en redes sociales, salvo que tengan el consentimiento de sus progenitores o tutores, resulta sencillo evitar dicha prohibición amparados en el anonimato, a lo que hay que añadir los escasos controles de verificación de edad, que, en muchos casos, se limitan a solicitar la fecha de nacimiento o a declarar la mayoría de edad. Por lo que, obviamente, los y las menores que quieren eludir la prohibición indican falsamente que son mayores de edad, con lo que pueden generar estos perfiles con gran facilidad, incluso pudiendo tener varios abiertos. En relación a esta problemática, el *Anteproyecto de Ley Orgánica para la protección de menores en el entorno digital*, que será analizado más adelante, plantea, entre otras, una serie de medidas como la verificación de edad para el acceso de menores a páginas de pornografía y la elevación de la edad de 14 a 16 años en la que pueden abrir perfiles en redes sociales.

Esta circunstancia implica un doble riesgo; por un lado, son más vulnerables a cualquier manipulación por parte de adultos con finalidades ilícitas. Los depredadores de niños y niñas a menudo emplean Internet para identificar a sus víctimas ganándose su confianza para dirigir su actividad a la recopilación, distribución y comercialización de imágenes de carácter sexual y obligar a sus víctimas, mediante el engaño y chantaje, a participar de actos sexuales, vídeos e imágenes que pueden ser vendidas o cedidas millones de veces sin tener que reponer el suministro. Por otro lado, los y las menores pueden tener acceso a contenidos inapropiados para su corta edad, puesto que en el entorno digital es más fácil acceder a información que promocione la violencia, los estereotipos de género, la discriminación, la pornografía y la explotación sexual. Según datos recogidos en la *Guía clínica sobre el ciberacoso para profesionales de la Salud*, un 40 % de los y las menores de entre 9 y 13 años disponen de una red social con un perfil propio, lo que permite concluir que, desde muy corta edad, tienen acceso. Se debe recalcar la necesidad de la educación digital y el acompañamiento para conseguir una navegación de forma segura y, que, de esta forma, sean conscientes de los desafíos a los que se enfrentan. Además, incidir en la búsqueda de mecanismos que faciliten el acceso de los y las menores al entorno digital en condiciones de seguridad, igualdad y gratuidad[134].

En cualquier caso, debemos evitar demonizar el acceso de los y las menores a Internet, puesto que las nuevas tecnologías les brindan un abanico de posibilidades muy positivas en relación con el ejercicio

---

133 GÓMEZ MIGUEL A., SANMARTÍN ORTÍ A., y KURIC KARDELIS S.; «Videojuegos y jóvenes: lugares, experiencias y tensiones», DOI: 10.5281/zenodo.7970990, 2023, pp. 70. Disponible en: https://drogodependencias.femp.es/sites/default/files/2023.Videojuegos-y-jovenes.Informe-final.pdf

134 SEPEAP. *Guía clínica sobre el ciberacoso para profesionales de la Salud*, 2015. Disponible en: https://sepeap.org/guia-clinica-sobre-el-ciberacoso-para-profesionales-de-la-salud/

de sus derechos civiles, culturales, educacionales, sociales y económicos y de formación de la propia identidad.

En suma, es trascendental el desarrollo y la puesta en marcha de líneas de actuación de prevención, concienciación y formación especializadas encaminadas a que las personas menores sepan detectar y advertir los riesgos inherentes de navegar por la red y, particularmente, en referencia a los contenidos para adultos y/o violentos.

CAPÍTULO III.
POLÍTICAS PÚBLICAS, LEYES Y NORMATIVA

1. CONTEXTUALIZACIÓN PRELIMINAR

En la actualidad, a la luz de lo dispuesto en el ámbito internacional y estatal, se hace necesaria la aplicación de la interpretación con perspectiva de género, que puede entenderse como un instrumento o medio de análisis de la realidad que pretende el poder explicar ciertos fenómenos. Así, la perspectiva de género permite identificar la asignación de roles distintos y desiguales aplicados a los hombres y a las mujeres a lo largo de la historia[135].

En realidad, la inclusión de la perspectiva de género en la elaboración y aplicación de todas las disposiciones jurídicas internacionales, europeas o estatales, constituye una manifestación del progreso en valores y en derechos de la sociedad internacional. Tal y como señala DÍEZ PERALTA, el establecimiento de garantías facilita la lucha frente a la discriminación, fenómeno que vulnera la dignidad humana[136].

Centrándonos en nuestro país, la Ley Orgánica 1/2004, de 28 de diciembre, de protección integral contra la violencia de género[137] marcó un cambio determinante en la lucha contra la violencia machista, ya que fue la primera norma que ofrece una protección global y transversal en todos los ámbitos, no sólo en el jurídico, sino también en el social, laboral, sanitario y educativo. Y, además, constituye un cambio de mentalidad, pues se comienza a calificar las agresiones en la pareja o expareja como manifestaciones de violencia contra las mujeres desde una perspectiva de carácter interdisciplinar[138]. Ciertamente, en atención al momento social de su aprobación, la norma no contempla referencias a la violencia digital, pero sí proporciona un marco legal apto para la implementación de programas contra la violencia de género digital. Sin embargo, en consonancia con las Propuestas del Parlamento Europeo y el Consejo de Europa, es recomendable incluir en la LO 1/2004 referencias a la violencia digital de forma expresa.

Otro hito histórico en España es la aprobación en 2017 del Pacto de Estado contra la Violencia de Género (PEVG), aprobado unánimemente por todos los grupos parlamentarios de las Cortes Generales. El

---

135 MANJÓN-CABEZA OLMEDA, A.; «La mujer víctima de la violencia de género. (Legislación penal y Sentencia del Tribunal Constitucional 59/2008, de 14 de mayo)», en MARTÍNEZ FRANCISCO, M. N., GARCÍA-PABLOS DE MOLINA, A., MIRANDA DE AVENA, C.; «Víctima, prevención del delito y tratamiento del delincuente». Granada, Comares, 2009. pp. 43-74.

136 DÍAZ PERALTA, E.; «*El matrimonio infantil y forzado en el Derecho internacional: Un enfoque de género y de derechos humanos»*, Valencia, Tirant lo Blanch, 2019, pp. 10-15.

137 LLORIA GARCÍA, P.; «La regulación penal en materia de violencia familiar y de género tras la Reforma de 2015. Especial referencia al ámbito tecnológico». *Revista General de Derecho Penal,* 2019, n.º 31, pp. 4-10.

138 YELA UCEDA, M.; «Estatuto de refugiada por motivos de género, blindaje de fronteras y desafíos actuales en la UE». *FEMERIS: Revista Multidisciplinar de Estudios de Género*, 2022, v. 7, n.º 2, pp. 142-157.

PEVG, que fue renovado en 2021, recoge el compromiso de todas las instituciones con la sociedad con el fin de avanzar en la erradicación de la violencia contra las mujeres en todas sus formas. Inicialmente, el PEVG abarca un total de 292 medidas estructuradas en 10 ejes de acción. Por su parte, la Delegación del Gobierno contra la Violencia de Género, bajo el Ministerio de Igualdad, ha elaborado un informe que evalúa las medidas implementadas durante los primeros cinco años de vigencia del Pacto (2018-2022), con el objetivo de identificar disfunciones, carencias y formular propuestas de mejora para seguir avanzando en la erradicación de la violencia contra las mujeres, considerada un grave atentado contra los derechos humanos.

En 2019, en relación con la ciberviolencia, el *Documento refundido de medidas del Pacto de Estado en materia de violencia de género. Congreso + Senado* contempla las siguientes medidas:

- Medida 34: Dar formación a los jóvenes sobre el uso adecuado y crítico de Internet y las nuevas tecnologías, especialmente en la protección de la privacidad y sobre los ciberdelitos (*stalking, sexting, grooming,* etc.).

  Esta iniciativa está en proceso de desarrollo, aunque ya hay varios textos legales que la mencionan. Por ejemplo, la Ley Orgánica 3/2018, del 5 de diciembre, sobre Protección de Datos Personales y garantía de los derechos digitales, establece la creación de un Plan de Actuación que busca promover acciones de formación, difusión y concienciación. El objetivo es que los menores utilicen de manera equilibrada y responsable los dispositivos digitales, las redes sociales y otros servicios de información en línea, asegurando así su adecuado desarrollo personal y la protección de su dignidad y derechos fundamentales (artículo 97.2).

  Asimismo, la Ley Orgánica 8/2021, del 4 de junio, que se centra en la protección integral de la infancia y la adolescencia frente a la violencia, menciona en su artículo 33 la importancia de formar al alumnado en un uso seguro y respetuoso de los medios digitales, alineado con la dignidad humana, los valores constitucionales y los derechos fundamentales, especialmente en lo que respecta a la intimidad personal y familiar y la protección de datos.

  Finalmente, el artículo 6 del Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en entornos digitales, subraya la necesidad de impulsar actividades que mejoren la competencia digital. Esto tiene como fin asegurar que los estudiantes se integren plenamente en la sociedad digital y aprendan a utilizar las tecnologías de manera segura, saludable, sostenible, crítica y responsable, tanto para su aprendizaje como para su participación social. Esta norma también destaca la importancia de la formación digital para que las personas menores de edad se conviertan en usuarios conscientes y seguros de la tecnología, considerando los aspectos psicológicos y el impacto emocional y cognitivo de sus experiencias en línea.

- Medida 42: Acordar, con las Fuerzas y Cuerpos de Seguridad del Estado, las empresas de telecomunicaciones y los principales proveedores de contenidos digitales, un sistema de coordinación, cooperación y corregulación para eliminar referencias potencialmente nocivas en la web que promuevan la violencia contra las mujeres.

Esta propuesta se encuentra en proceso de desarrollo, puesto que con la entrada en vigor de la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, se establecen una serie de obligaciones en relación con el ámbito digital y de la comunicación en la prevención de las violencias sexuales (art. 10). Fomentar medidas como acuerdos con prestadores de servicios, formación del personal de medios de comunicación y adopción de acuerdos de autorregulación. Estos mecanismos buscan prevenir conductas de apología de violencias sexuales, capacitar al personal para informar con objetividad y respeto a las víctimas, y sensibilizar sobre la importancia de prevenir estas violencias. Se enfatiza en la libertad de expresión, la independencia y la libre prestación de servicios, así como en el respeto a la dignidad y derechos de las víctimas.

Por otra parte, se ha dado a conocer el Acuerdo del Consejo de Ministros de julio de 2021, a través de la Resolución emitida por la Subsecretaría, en el que se aprueba el Catálogo de Medidas Urgentes del Plan de Mejora y Modernización contra la Violencia de Género. Este Catálogo contiene diversas medidas destinadas a fortalecer y revisar la respuesta institucional ante la violencia de género. Dentro de estas medidas, la número 2 tiene como objetivo promover acuerdos de colaboración con las principales proveedoras de servicios en línea para prevenir y abordar los perfiles que promueven la discriminación y la violencia contra las mujeres. Además, busca garantizar un tratamiento adecuado de las noticias e información relacionada con la violencia de género ofrecida por los diferentes medios de comunicación, así como evitar la representación «cosificada» de la mujer en la publicidad.

- Medida 44: Garantizar que la concesión de sellos de calidad no recaiga en los sitios web con contenidos digitales potencialmente nocivos que promuevan la violencia contra las mujeres.

  Este objetivo ha sido cumplido. Según el artículo 12 de la Ley Orgánica 10/2022, las empresas que se adapten a lo establecido en esta normativa recibirán el distintivo de «Empresas por una sociedad libre de violencia de género», el cual podrá ser retirado en caso de circunstancias que así lo requieran. Se asegura que este distintivo no será otorgado a sitios web con contenidos que fomenten la violencia contra las mujeres. Además, se establece que, mediante un Real Decreto, se determinará el proceso para la concesión, revisión y retirada de este distintivo, así como las facultades y condiciones relacionadas con su obtención y difusión institucional. En este sentido, en 2023 se aprueba el Real Decreto 333/2023, que modifica el Real Decreto 1615/2009, regulando el distintivo «Igualdad en la Empresa».

- Medida 102: Ampliar el concepto de violencia de género a todos los tipos de violencia contra las mujeres contenidos en el Convenio de Estambul.

  Igualmente, acatada esta medida, ya que la Ley Orgánica 10/2022 y la Estrategia Estatal para combatir las violencias machistas 2022-2025 amplían el concepto de violencia de género a todos los tipos de violencia contra las mujeres establecidos en el Convenio de Estambul, tanto desde la perspectiva legislativa como en el ámbito de las políticas públicas. Esta Ley Orgánica destaca, en

su artículo 3, la importancia de abordar las violencias sexuales en el ámbito digital, incluyendo la difusión de actos de violencia sexual, la pornografía no consentida y la pornografía infantil, así como la extorsión sexual a través de medios tecnológicos.

- Medida 109: Perfeccionar la tipificación de los delitos en el ámbito digital.

  Cumplida la medida, puesto que el derecho penal español ha mejorado la protección de los derechos y garantías en el ámbito digital mediante la introducción de nuevas normativas. La Ley Orgánica 8/2021 incluye nuevos tipos penales para combatir conductas realizadas a través de medios tecnológicos que pongan en riesgo a las personas. Por otro lado, la Ley Orgánica 10/2022 tipifica delitos como la utilización de la imagen de una persona sin consentimiento para crear perfiles falsos en redes sociales, entre otros. Estas leyes también permiten la retirada de contenidos ilícitos de la red para prevenir un mayor daño. La modificación del Código Penal en el artículo 189 bis por la Ley Orgánica 4/2023 refuerza la penalización de la distribución de contenidos que promuevan delitos a través de Internet y otras tecnologías.

- Medida 112: No considerar las injurias y calumnias a través de las redes sociales en el ámbito de la violencia de género como únicamente un delito leve.

  Según la reforma del Código Penal realizada por la Ley Orgánica 1/2015, sólo se consideran delito las injurias que sean consideradas graves por el concepto público. Sin embargo, el delito leve de injurias sólo es punible en casos de violencia de género, según el artículo 173. Para abordar las injurias y calumnias en medios de comunicación social, es necesario revisar la reforma anterior del Código Penal. Actualmente, esta medida se encuentra en proceso, tras la reforma del Código Penal realizada por la Ley Orgánica 10/2022, que implica una mejora en la protección de las mujeres frente a la violencia de género en el ámbito digital. Incluye un nuevo apartado en el artículo 172 ter, que castiga el acoso a una persona de manera persistente y reiterada, así como el uso indebido de datos personales. También se penaliza el uso de la imagen de una persona sin su consentimiento para acosarla, hostigarla o humillarla. Además, se modifica el artículo 197 para penalizar la difusión de imágenes o grabaciones obtenidas sin permiso en un lugar privado, especialmente cuando atenta contra la intimidad de la persona afectada. Las penas aumentan en casos específicos, como cuando los hechos son cometidos por familiares cercanos, sobre personas menores de edad o personas con discapacidad.

- Medida 143: Establecer como medida cautelar y como pena privativa de derechos, la prohibición de comunicarse a través de las redes sociales cuando el delito se cometa a través de las nuevas tecnologías.

  Este objetivo está en proceso. El Anteproyecto de Ley Orgánica para la protección de los menores en entornos digitales incluye la medida de alejamiento de los espacios virtuales, con el objetivo de fortalecer la prevención tanto general como específica en relación con los delitos tecnológicos. Específicamente, se realizarán modificaciones en los artículos 33, 39, 40, 45, 48,

56, 70 y 83 del Código Penal para establecer la prohibición de acceso o comunicación a través de redes sociales, foros, plataformas de comunicación y otros espacios virtuales, en los casos en que se cometa un delito en esos entornos. Esta nueva medida busca ofrecer una respuesta efectiva ante el aumento de la criminalidad informática, evitando la repetición de conductas delictivas en el ámbito digital y mejorando la protección de las víctimas, al prevenir su revictimización.

Además, para potenciar la seguridad de las víctimas, la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, introduce un nuevo párrafo en el artículo 13 de la Ley de Enjuiciamiento Criminal, el cual establece que en la investigación de delitos perpetrados a través de Internet, el teléfono u otras tecnologías de la información y la comunicación, el tribunal podrá ordenar como primeras medidas cautelares, de forma voluntaria o a petición de parte, la retirada provisional de contenidos ilícitos, la suspensión temporal de los servicios que presenten dichos contenidos o el bloqueo temporal de ambos cuando se encuentren en el extranjero.

Cabe indicar que, en marzo de 2024, se han iniciado los trabajos de renovación y actualización del Pacto de Estado, mediante la creación de una subcomisión, que dispondrá hasta diciembre del mismo año para acometer esta renovación. El Ministerio de Igualdad ha propuesto incorporar la violencia digital, así como la lucha contra el acceso de menores a la pornografía y la prostitución, entre las medidas a analizar.

Por otra parte, es preciso mencionar que el Tribunal Europeo de Derechos Humanos (TEDH) ha emitido diferentes resoluciones en relación con los delitos cometidos mediante Internet, aunque sólo una sentencia se ha ocupado de vincular la violencia digital con la violencia de género (Buturugâ *vs.* Rumanía), fallo que examinaremos posteriormente. Algunos ejemplos son:

1. Caso MTE y otros *vs*. Hungría (2016). Obligación del Estado de proteger a los niños de la explotación sexual en línea. El Tribunal sostuvo que los Estados deben tomar medidas efectivas para prevenir y sancionar la explotación sexual de menores en Internet, incluso a través de la cooperación internacional y la legislación adecuada.
2. Caso Delfi AS *vs*. Estonia (2015). Abordó la responsabilidad de los sitios *web* por los comentarios difamatorios publicados por usuarios. El Tribunal estableció que los sitios *web* pueden ser considerados responsables si no toman medidas razonables para prevenir o eliminar contenido difamatorio, incluso en el contexto de los comentarios en línea.
3. Caso S.K. *vs.* Alemania (2010). Trató el ciberacoso en el contexto de la protección de menores. El Tribunal sostuvo que los Estados tienen la obligación de proteger a los menores de la violencia en línea, incluyendo el acoso. Se estableció que los Estados deben tomar medidas efectivas para prevenir y sancionar el ciberacoso y garantizar la protección de los derechos de los menores.
4. Caso Lliya Stefano *vs.* Bulgaria (2008). En el que se discutía si el registro del despacho de un abogado y de sus datos físicos y electrónicos suponía una injerencia en el derecho a la intimidad y qué presupuestos eran necesarios para que la intervención policial se considerase legítima, requiriendo habilitación judicial para cualquier injerencia en el contenido de un ordenador personal.

5. Casos acumulados Riley *vs.* California y EE. UU. *vs*. Brima Wurie-573 U.S. (2014). En estos, se reflejaba la gravísima afectación de la privacidad que podía derivarse de un examen indiscriminado y sin límites de un teléfono inteligente.

Deteniéndonos en el Caso Buturugâ *vs*. Rumanía (2020), como hemos comentado, el TEDH reconoce por primera vez el ciberacoso como una forma de violencia contra la mujer y que puede adoptar múltiples maneras en relación con la violación de la privacidad vinculada al uso de las TIC. En el contexto de la Convención Europea de Derechos Humanos, el Tribunal analiza la posible vulneración de los artículos 3 y 8, que prohíben la tortura y los tratos inhumanos o degradantes, así como garantizan el derecho al respeto de la vida privada y familiar. Dentro de la argumentación del Tribunal, se debe señalar que el fallo de este caso considera que no hubo una respuesta efectiva e idónea en relación con la investigación y la diligencia requerida para la situación de riesgo manifestada por la demandante. Como critica la resolución, hay que decir que elude mencionar expresamente la situación de quebrantamiento de condena, la sensación de impunidad que esta falta de respuesta de las autoridades provocó en el agresor y en la víctima y, también, que evita considerar esta situación como parte de una violencia de control.

Además, el TEDH, a pesar de reconocer la ciberviolencia como una clase de violencia de género, lo hace de una manera muy limitada. No entra en profundidad en el examen de ese maltrato dentro de una situación de sometimiento, temor y agresión a la mujer; es decir, no la enmarca dentro del concepto de tortura del artículo 3, sino exclusivamente como ciberatentado a la intimidad vinculado con el derecho al secreto de las comunicaciones.

En cualquier caso, confiamos que esta sentencia sirva de guía para que el Tribunal adopte nuevas resoluciones con perspectiva de género y relacione la idea de violencia contra las mujeres con un carácter integral del fenómeno y facilite una mejor protección a las víctimas.

A continuación, vamos a revisar la normativa a nivel europeo, estatal y autonómico que expresamente hacen mención a la violencia digital para determinar como está plasmada esta violencia en los marcos normativos y legislativos.

2. POLÍTICAS PÚBLICAS, LEYES Y NORMATIVA EN EL MARCO EUROPEO

En el marco europeo, existen leyes y normas específicas de ciberviolencia, sin regular específicamente la violencia digital de género ni hacia las personas menores de edad. Por otro lado, nos encontramos políticas públicas que recogen este tipo de violencia como una tipología propia dentro de la normativa.

A continuación, en primer término, vamos a analizar las normas centradas en el entorno digital. Seguidamente, aquellas enfocadas en la violencia de género y personas menores de edad que hacen mención al entorno digital.

2.1. *Convenio del Consejo de Europa sobre la Ciberdelincuencia*

El Convenio del Consejo de Europa sobre la Ciberdelincuencia, conocido como Convenio de Budapest, se celebra el 23 de noviembre de 2001 en Budapest con el objetivo de incrementar la cooperación

internacional y generar marcos legales acordes entre las naciones para luchar contra la criminalidad a través de la red[139].

Es el primer tratado internacional jurídicamente vinculante en materia de ciberdelincuencia, auxilio internacional y pruebas electrónicas. Los Estados parte deberán fortalecer su derecho procesal penal interno y reforzar el sistema penal privilegiando la reparación del daño a la víctima en relación con la obtención de pruebas electrónicas, cooperación internacional e investigación y enjuiciamiento de la ciberdelincuencia y otros delitos que conlleven prueba electrónica. Igualmente, mediante una serie de disposiciones de Derecho penal sustantivo, aborda directa e indirectamente algunos tipos de violencia contra las mujeres en línea y facilitada por la tecnología y, junto con sus protocolos adicionales, representan un marco muy interesante para reflexionar sobre el fenómeno, en relación con el Convenio de Estambul.

Con respecto a esta última cuestión, algunos artículos se relacionan con la violencia en línea, como el ciberacoso, mientras que otros refieren actos que podrían estar vinculados con este problema, pero de manera menos directa. Por ejemplo, el artículo 2 aborda el acceso ilegal al sistema de la víctima, común en las ciberamenazas y ciberviolencia. El artículo 3 se refiere a la vigilancia del contenido de las comunicaciones para obtener o grabar datos personales de la víctima, con la instalación de *sotfware* o el empleo de piratería informática, lo cual puede facilitar el ciberacoso. Por su parte, el artículo 8 permite la posibilidad de vincular los casos de fraude informático, descritos en el artículo, con el fenómeno de la sextorsión, debido a que los delincuentes pueden utilizar información privada para chantajear a la víctima exigiendo dinero, a menudo utilizando tácticas de pirateo. Por otra parte, los artículos 16 a 21 detallan las medidas que las Partes deben tomar en la obtención de pruebas electrónicas en procedimientos penales. El Convenio de Budapest busca mejorar la persecución de delitos en línea, acelerando la asistencia mutua en materia penal y facilitando el acceso a pruebas electrónicas[140].

El Tratado sirve de guía para cualquier país que legisle contra la ciberdelincuencia y todos los delitos que lleven implícitas pruebas electrónicas.

El Convenio y su Informe explicativo[141] fueron adoptados por el Comité de Ministros del Consejo de Europa en noviembre de 2001, con motivo de la celebración de la Conferencia Internacional sobre la Ciberdelincuencia y entró en vigor el 1 de julio de 2004. Fue ratificado por España en junio de 2010, entrando en vigor el 1 de octubre de 2010, conforme a lo establecido en su artículo 36.4.

En el texto se exige a las Partes la penalización de los delitos perpetrados contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos o por medio de ellos; de los delitos

---

139 CONSEJO DE EUROPA. Convenio sobre la Ciberdelincuencia (ETS n.º 185) Referencia RCDE n.º 185 de 23 de noviembre de 2001, Budapest. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

140 CONSEJO DE EUROPA. *Proteger a las mujeres y niñas de la violencia en la era digital. La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología*, 2021. Disponible en: https://edoc.coe.int/en/violence-against-women/11280-proteger-a-la-mujeres-y-ninas-de-la-violencia-en-la-era-digital.html

141 CONSEJO DE EUROPA. Convenio sobre la Ciberdelincuencia (ETS n.º 185) Referencia RCDE n.º 185 de 23 de noviembre de 2001, Budapest. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

relacionados con el contenido concernientes a la producción, difusión o posesión de materiales de abuso sexual de niños y niñas, del acoso y de las infracciones de los derechos de propiedad intelectual.

Asimismo, los Estados parte del Convenio se comprometen a reforzar sus competencias en cuanto al derecho procesal penal interno y dotar a su sistema judicial de los medios necesarios para obtener pruebas electrónicas en relación con cualquier delito.

Cada vez son más los países adheridos. En febrero de 2024 eran sesenta y nueve Estados[142], entre los que se encuentran países europeos, así como Argentina, Australia, Brasil, Cabo Verde, Camerún, Canadá, Chile, Colombia, Costa Rica, Estados Unidos, Filipinas, Ghana, Israel, Japón, Marruecos, Mauricio, Nigeria, Panamá, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal y Tonga. Otros dos lo han firmado, Irlanda y Sudáfrica y otros veintidós Estados han sido invitados a adherirse: Benín, Burkina Faso, Costa de Marfil, Ecuador, Corea, Fiyi, Granada, Guatemala, Kazajstán, Kiribati, México, Mozambique, Nueva Zelanda, Níger, Ruanda, Santo Tomé y Príncipe, Sierra Leona, Timor Oriental, Trinidad y Tobago, Túnez, Uruguay y Vanuatu[143].

El Comité de Seguimiento y Oficina del Programa contra la Ciberdelincuencia (T-CY) vela por la aplicación efectiva del Convenio de Budapest y representa a los Estados parte en el mismo. El artículo 46 del Convenio define las funciones del Comité. El T-CY facilita el uso y la aplicación efectivos del Convenio, favorece el intercambio de información pertinente entre las Partes en el ámbito de la ciberdelincuencia y la obtención de pruebas en formato electrónico y, por último, es responsable de preparar las posibles enmiendas al Convenio.

Como complemento a la labor del T-CY se ha creado la Oficina del Programa de Lucha contra la Ciberdelincuencia del Consejo de Europa (C-PROC) en Bucarest, Rumanía. La tarea de C-PROC es dotar a los países de todo el mundo de los medios necesarios para fortalecer la capacidad de sus sistemas legales para responder a los desafíos que entrañan los delitos cibernéticos y las pruebas electrónicas, tanto en el ámbito nacional como internacional. C-PROC se centra específicamente en asesorar a los Estados en la redacción de nuevas leyes, o en su actualización, sobre la base del Convenio de Budapest y las normas conexas. Incluye soporte para:

1. Fortalecer la legislación sobre delitos cibernéticos y pruebas electrónicas en consonancia con las normas del estado de derecho y los derechos humanos (incluida la protección de datos).

---

142 CONSEJO DE EUROPA. Convenio sobre la Ciberdelincuencia (ETS n.º 185) Referencia RCDE n.º 185 de 23 de noviembre de 2001, Budapest. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

143 Ibidem. Vid., artículo 37:
«1. A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitan a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará respetando la mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de Ministros. 2. Para todo Estado que se adhiera al Convenio de conformidad con el párrafo 1 precedente, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa».

2. Capacitar a jueces, fiscales y agentes del orden.
3. Establecer unidades especializadas en delitos cibernéticos y forenses y mejorar la cooperación entre agencias.
4. Promocionar la cooperación público-privada.
5. Proteger a los niños contra la violencia sexual en línea.
6. Mejorar la eficacia de la cooperación internacional.

C-PROC, con su función de desarrollo de capacidades, complementa el trabajo del Comité de la Convención sobre Delitos Cibernéticos T-CY, a través del cual los Estados parte siguen la implementación de la Convención de Budapest.

El Consejo de Europa puede apoyar a cualquier país en el fortalecimiento de su legislación nacional en materia de ciberdelincuencia. La adhesión de un gobierno al Convenio de Budapest representa un compromiso político y permite brindar todo tipo de asistencia para reforzar las capacidades de la justicia penal. C-PROC obra también para proteger a los niños y las niñas contra la violencia sexual en línea y, a través de una serie de actividades sobre la violencia cibernética, explora las sinergias entre el Convenio de Estambul y el Convenio de Budapest, así como otros instrumentos.

El 1 de marzo de 2006 entró en vigor el Primer Protocolo Adicional al Convenio sobre la Ciberdelincuencia. Los estados que lo han ratificado deben penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como amenazas racistas y xenófobas e insultos. Se pretende evitar la impunidad de los delincuentes y abordar de manera más completa y efectiva la problemática de la instigación al odio por medios electrónicos.

Para complementar el Convenio de Budapest y su Primer Protocolo, en septiembre de 2017 comenzó la preparación del Segundo Protocolo Adicional[144], con el que se aspira a desarrollar, seguir mejorando y reforzar la utilización de las herramientas de cooperación para la obtención de evidencias electrónicas en otros países distintos de aquel que las necesita para una investigación. Y no sólo con otros países, sino con los proveedores de servicios y otras entidades que dispongan de la información necesaria para la identificación de los agresores. Se trata de, mediante instrumentos adicionales relacionados, conseguir una asistencia mutua más eficiente y otras formas de colaboración entre autoridades, como cooperación en emergencias (donde exista un riesgo importante e inmediato para la vida o seguridad de cualquier persona física). Igualmente, se pretende establecer una cooperación con los proveedores de servicios y entidades que disponen de la información pertinente. En este proyecto han trabajado intensamente representantes de un gran número de países miembros de la Convención. España ha participado de forma muy activa mediante la intervención de representantes del Ministerio de Justicia, Fuerzas y Cuerpos de Seguridad (CNP y Guardia Civil) y la Fiscalía en materia de Criminalidad Informática. Y el 12 de mayo de 2022, nuestro país firmó este Segundo

[144] DOUE. *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas*, 2023. Disponible en: https://www.boe.es/buscar/doc.php?id=-DOUE-L-2023-80291

Protocolo Adicional, que había sido adoptado por el Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021. Más adelante en el apartado del estudio centrado en los problemas transfronterizos de la violencia digital ahondaremos en este Segundo Protocolo Adicional en relación a dicha cuestión.

Con la finalidad de implementar el Convenio de Budapest y sus Protocolos, en diciembre de 2023 se celebró la 14ª edición de la Conferencia Octopus en Bucarest. En este encuentro participaron alrededor de 500 profesionales especialistas en ciberdelincuencia de más de cien países, junto con organizaciones internacionales y del sector privado, sociedad civil y del mundo académico. Se trata de un espacio de intercambio de conocimientos y experiencias en materia de ciberdelito entre los asistentes, que destaca por la calidad de los ponentes que participan en ella. Es un proyecto del Consejo de Europa basado en contribuciones voluntarias de los Estados parte y Observadores de la Convención sobre la Ciberdelincuencia y otras organizaciones del sector público y privado. El Proyecto se desarrolla entre el 1 de enero del 2021 y el 31 de diciembre de 2027 y se espera que ofrezca resultados en las siguientes áreas:

1. Asistencia de las autoridades de justicia penal de los países dispuestos a implementar el Convenio de Budapest, su Primer Protocolo sobre Xenofobia y Racismo, su Segundo Protocolo Adicional al Convenio sobre Delito Cibernético y mayor cooperación y divulgación de evidencia electrónica, así como estándares relacionados.
2. Apoyo al Comité de la Convención sobre Delitos Cibernéticos T-CY.
3. Organización de las conferencias Octopus sobre cooperación contra la ciberdelincuencia.
4. Desarrollo de herramientas en línea para la capacitación sobre delitos cibernéticos y evidencia electrónica.

En relación con el ciberacoso, en la Conferencia se han adoptado diversas medidas y propuestas para prevenir y combatir este problema. Algunas de estas incluyen la creación de programas de concienciación sobre ciberacoso en escuelas y comunidades, el fortalecimiento de la legislación contra el acoso en línea y la promoción de plataformas y herramientas seguras para denunciar incidentes de ciberacoso.

Asimismo, se han discutido reflexiones sobre la importancia de involucrar a los actores de la sociedad en la lucha contra el ciberacoso, desde los gobiernos y empresas tecnológicas hasta los usuarios de Internet. Se ha destacado la necesidad de trabajar de manera colaborativa para abordar este problema y proteger a las personas, especialmente a los más vulnerables como los niños, las niñas y adolescentes.

La Conferencia Octopus supone un espacio importante para generar conciencia y plantear soluciones efectivas[145].

---

[145] CONSEJO DE EUROPA. *Conferencia regional sobre ciberviolencia y pruebas electrónicas. América Latina y el Caribe.* Enmarcada en los Proyectos Octupus y Glacy+, 2021. Disponible en: https://rm.coe.int/2542-37-regconf-cyberviolence-26-27-nov-2021-summary-report-es/1680a57a13

2.2. *Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales*

El 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 es la primera norma en el ámbito digital que obliga a las empresas de servicios digitales de la Unión Europea a rendir cuentas por los contenidos publicados en sus plataformas.

Este Reglamento (también conocido como Ley de Servicios Digitales), aprobado en 2022 y en vigor desde febrero de 2024, se centra en la protección de los derechos fundamentales en el entorno digital. Pretende combatir contenidos ilícitos, tales como la incitación al odio, acoso y abuso a menores, noticias o propaganda falsa y reaccionar rápidamente ante ellos. Con esta finalidad, establece la prohibición de mostrar publicidad personalizada basada en la utilización de sus datos personales a las plataformas abiertas a menores. Además, a las plataformas en línea de gran tamaño (VLOP)[146] (p. ej., *Facebook, Instagram, TikTok, Snapchat, YouTube*, etc.) se les establecen un conjunto de medidas cuyo objetivo es proteger mejor al consumidor y sus derechos fundamentales *online*, así como luchar contra contenidos ilícitos y otorgar mayor transparencia y garantía de un «*mercado único y uniforme en la UE*». Entre otras, deben contar con dispositivos que identifiquen rápidamente contenidos ilegales para su retirada. A su vez, estas plataformas deberán combatir la desinformación para ofrecer una completa protección de los y las menores, así como luchar contra la violencia de género. Y, al mismo tiempo, las plataformas de gran tamaño deben responder a los criterios de transparencia y buen gobierno. En caso de incumplimiento de la normativa, se exponen a sanciones económicas que pueden llegar hasta el 6 % de su volumen de la cifra de negocio mundial.

2.3. *Propuesta de Directiva 2024/2486 del Parlamento Europeo y del Consejo por la que se establece un paquete normativo para prevenir y combatir el abuso sexual de los menores en el entorno digital*

El objetivo de esta Propuesta de Directiva europea es garantizar que todos los proveedores de servicios en línea y plataformas de Internet que operen en la Unión Europea detecten, notifiquen y eliminen de manera obligatoria cualquier material relacionado con abuso sexual infantil, así como mejorar los mecanismos de prevención. Esto incluye la formación especializada del personal de estos proveedores de servicios y la implementación de cursos de prevención en centros educativos para que los menores puedan identificar los riesgos asociados.

Otras medidas incluyen la eliminación inmediata de contenido de este tipo, la verificación de la identidad de los usuarios para proteger a las personas menores, la prohibición de compartir mensajes o imágenes en tiempo real en juegos en línea, y la notificación a las autoridades en caso de identificar posibles casos de abuso sexual. Además, se prestará atención a contenido generado por IA.

---

[146] Las plataformas en línea se consideran de gran tamaño si tienen más de 45 millones de personas usuarias. (VLOP es la abreviatura de *«Very Large Online Platforms»).* Estos servicios tendrán 4 meses para cumplir con las obligaciones de la DSA, que incluye realizar y proporcionar a la Comisión su primera evaluación de riesgos anual. Los Estados miembros de la UE deberán nombrar coordinadores de servicios digitales antes del 17 de febrero de 2024, cuando también las plataformas con menos de 45 millones de usuarios activos deberán cumplir con todas las reglas de la DSA.

El artículo 16 de la norma regula el derecho a la integridad y dignidad de los menores, indicando que las empresas proveedoras de servicios en línea deben tomar medidas proactivas para evitar y combatir el ciberacoso, la explotación sexual y cualquier otro tipo de contenido perjudicial que pueda afectar la integridad y dignidad de los menores. Asimismo, es fundamental implementar políticas de uso seguro, herramientas de denuncia y moderación de contenido y promover una cultura de respeto y empatía en línea.

Por último, se creará el Centro Europeo de prevención y combate del abuso sexual de menores en línea para apoyar los objetivos de la directiva, mediante la coordinación de acciones entre los Estados miembros, la recopilación de datos y de buenas prácticas y persecución de casos. Impulsará el desarrollo de nuevas tecnologías y herramientas para la detección, prevención y respuesta al abuso sexual de personas menores en línea.

2.4. *Directiva 2013/40/UE del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información*

Esta Directiva[147] de 12 de agosto de 2013, que sustituye la Decisión marco 2005/222/JAI del Consejo, establece normas mínimas relativas a la definición de las infracciones penales y a las sanciones aplicables en el ámbito de los ataques contra los sistemas de información. También tiene por objeto facilitar la prevención de dichas infracciones y la mejora de la cooperación entre las autoridades judiciales y otras autoridades especializadas competentes, como Eurojust, Europol y su Centro Europeo contra la Ciberdelincuencia y la Agencia Europea de Seguridad de las Redes y de la Información.

Implica que el método de protección de los sistemas de información deberá ser completo y abarcar múltiples aspectos, como la seguridad de los datos, la protección frente a ataques cibernéticos y la previsión de comportamientos delictivos que acompañen a las respuestas penales. Obviamente resulta de interés, puesto que la intromisión y robo de datos es el paso previo para la comisión de múltiples acciones incardinables en la idea de ciberviolencia.

2.5. *Reglamento de Inteligencia Artificial*

Recientemente, en marzo de 2024, el Parlamento Europeo ha aprobado la primera normativa completa sobre inteligencia artificial[148], que contó con el apoyo de todos los países miembros de la Unión Europea. Su principal objetivo es garantizar la protección de los derechos fundamentales de

---

147 UE. DIRECTIVA 2013/40/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Disponible en: https://www.boe.es/doue/2013/218/L00008-00014.pdf

148 PARLAMENTO EUROPEO. *Reglamento de Inteligencia Artificial. Resolución legislativa del PARLAMENTO EUROPEO, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión (COM (2021) 0206-C9-0146/2021-2021/0106 (COD)).* Disponible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

las personas, al mismo tiempo que fomenta la innovación y buscar posicionar a Europa como líder en este ámbito.

Con referencia a la obtención de datos por parte de los sistemas de IA, el Reglamento los ha clasificado como de alto y bajo riesgo, entendiendo que aquellos catalogados como de alto riesgo son merecedores de una protección reforzada. En este sentido, herramientas de reconocimiento biométrico, la captación de imágenes, los sistemas de recogida de huellas y/o ADN, son clasificados como de alto riesgo debido a que contienen datos sensibles que, de no estar supervisados, pueden usarse para suplantar la identidad. Se definen como de alto riesgo, puesto que en ellos existe un determinado «*desequilibrio de poder y pueden dar lugar a la vigilancia, la detención o la privación de libertad de una persona física»*[149]. Igualmente, la norma establece límites en el uso de esta identificación biométrica, prohíbe el uso de la IA para manipular o explotar las vulnerabilidades de los usuarios, y otorga derechos a los y las consumidoras para presentar quejas y recibir explicaciones.

Por lo que respecta a la responsabilidad, en estos casos se parte de que, a día de hoy, la responsabilidad de los sistemas de IA recae sobre el creador de las aplicaciones en cuestión, puesto que no existe una IA completamente autónoma. De ahí la necesidad que se establece por parte de la UE de la supervisión humana en los sistemas de IA calificados de alto riesgo, para evitar vulneraciones de derechos de las personas[150].

La norma pretende, entre otras cosas, que los sistemas de inteligencia artificial sean desarrollados y utilizados de manera inclusiva, promoviendo la igualdad de acceso, la igualdad de género y la diversidad cultural, y evitar cualquier efecto discriminatorio o sesgo injusto prohibido por la ley nacional o de la Unión Europea. Los conjuntos de datos utilizados en el entrenamiento, validación y prueba de los sistemas de inteligencia artificial de alto riesgo deberán estar sujetos a prácticas de gobernanza y gestión de datos adecuadas para el propósito previsto.

Precisamente por ello, considera de alto riesgo a los sistemas de inteligencia artificial utilizados para evaluar la calificación crediticia o solvencia de los individuos, ya que determinan su acceso a recursos financieros y servicios esenciales como la vivienda, la electricidad y las telecomunicaciones. Estos sistemas podrían discriminar a ciertas personas o grupos y perpetuar patrones históricos de discriminación fundamentados en el origen racial o étnico, en el género, en la situación de discapacidad, en la edad o la orientación sexual, o incluso generar nuevas formas de discriminación, en atención a las capacidades tecnológicas o algunas que aún no podamos imaginar.

En idéntico sentido, por ejemplo, la norma señala que los sistemas de IA aplicados en educación, si son empleados de manera inadecuada, podrían ser marcadamente intrusivos y vulnerar el derecho a la educación y a la formación, incluso pueden llevar a perpetuar patrones históricamente discriminatorios, por ejemplo, en las mujeres, en determinados grupos de edad y de personas con discapacidad o de concreto origen racial u orientación sexual. Por tanto, es importante promover la formación digital de alta calidad, que el alumnado comparta capacidades y competencias, capacitación mediática y desarrollo del pensamiento crítico.

---

149 Ibidem.

150 Ibidem. Vid., art. 26.

Igualmente, el uso de la IA en el campo laboral durante los procesos de contratación, evaluación, promoción o retención de personas, debe garantizar los derechos fundamentales de protección de datos y la privacidad de las personas, así como eludir la perpetuación de sesgos discriminatorios.

En mayo de 2024, en paralelo a la aprobación del Reglamento, la Comisión Europea presentó la estructura de la nueva Oficina de Inteligencia Artificial, que comenzará a operar a partir de junio. Este organismo desempeñará un papel fundamental en la implementación de la Ley de Inteligencia Artificial. Su objetivo será fomentar la investigación y la innovación en el campo de la IA fiable, se encargará de garantizar la uniformidad en la aplicación de la mencionada Ley, brindando apoyo a los órganos gubernamentales de los Estados miembros y colaborará estrechamente con el Consejo Europeo de Inteligencia Artificial, el cual está integrado por representantes de los Estados miembros.

2.6. *Código de Conducta para la lucha contra la incitación ilegal al odio en Internet*

Existen también otros instrumentos[151], acuerdos y políticas internacionales y regionales que tratan más específicamente la cuestión de la violencia contra las mujeres en línea y facilitada por la tecnología[152]. El Código de Conducta de la UE es uno de esos instrumentos.

Para prevenir y contrarrestar la propagación del discurso de odio ilegal en línea, en mayo de 2016 la Comisión Europea acordó con *Facebook, Twitter* y *YouTube* un «Código de Conducta». A lo largo de 2018, *Instagram*, *Snapchat y Dailymotio*n lo subscribieron. *Jeuxvideo.com* en 2019, *TikTok* en 2020 y *Linkendln* en 2021. En mayo y junio de 2022, respectivamente, *Rakuten viber* y *Twitch* anunciaron su participación en este Código. De acuerdo con la Comisión, aunque ya existe legislación europea relativa a la lucha contra el racismo y la xenofobia,

> «*las sanciones penales aplicadas por los Estados miembros a las personas que cometen actos de incitación al odio debe complementarse con el examen diligente por parte de las plataformas sociales de los casos de incitación ilegal al odio, reportados por los usuarios*».

El objetivo: reducir el plazo que tardan estas plataformas en retirar contenidos de odio de sus redes.

Al firmar este acuerdo voluntario, estas empresas se comprometieron a poner en marcha mecanismos internos que garantizasen el examen y la retirada de las manifestaciones que considerasen de incitación ilegal al odio en un plazo inferior a las 24 horas. Para lograr este objetivo, se preveían diversas medidas: por un lado, educar y sensibilizar a su personal y a las personas usuarias sobre los tipos de contenidos no autorizados; y, por otro lado, asegurar que los contenidos que se eliminasen fueran ilegales, gracias al contacto directo con una red de *«expertos/as de confianza»* pertenecientes

---

151 ONU. *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*, 2018. Disponible en: https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F38%2F47&Language=E&DeviceType=Desktop&LangRequested=False

152 UE. RECOMENDACIÓN (UE) 2018/334 DE LA COMISIÓN de 1 de marzo de 2018 sobre medidas para combatir eficazmente los contenidos ilícitos en línea. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32018H0334&from=FR

a la sociedad civil, creada específicamente para apoyar a estas compañías a resolver dudas acerca de la ilegalidad de los contenidos.

Además, también se comprometieron a compartir con los Estados miembros informes periódicos sobre el funcionamiento del mecanismo de reporte y la resolución de los casos notificados; a cooperar con la UE en el desarrollo e implementación de campañas de «*contra discurso*», y a promover la adhesión de otras plataformas sociales y empresas de medios de comunicación a este Código. Estos informes periódicos de seguimiento, establecidos en colaboración con una red de organizaciones ubicadas en los diferentes países de la Unión Europea y con una metodología comúnmente acordada, determinan el grado de implementación del Código de Conducta.

La séptima evaluación del Código de Conducta para combatir el discurso de odio ilegal en línea muestra que, en general, las empresas de tecnologías de la información eliminaron el 63,6 % del contenido que se les notificó, mientras que el 36,4 % permaneció en línea. Entre los motivos denunciados de discurso de odio, los más comunes son: el antigitanismo, la xenofobia y la orientación sexual, siendo destacable que el 4,1 % se refiere a causas de género[153].

2.7. *Directiva 2024/1385 del Parlamento Europeo y del Consejo, sobre la lucha contra la violencia contra las mujeres y violencia doméstica*

La Eurocámara aprobó, por amplia mayoría, el 24 de abril de 2024, la primera Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica[154]. Se trata de la primera normativa europea contra la violencia de género desde un punto de vista general y también específica en cuestiones relativas a la ciberviolencia. Su entrada en vigor será 20 días después de su publicación en el Diario Oficial de la Unión Europea y los Estados tendrán tres años para transponerla[155].

La normativa tiene dos partes claramente diferenciadas: por un lado, trata de establecer medidas de protección, apoyo, acompañamiento y colaboración entre Estados y, por otra, exige la tipificación de diferentes delitos, entre los que se encuentran la mutilación genital femenina o el matrimonio forzado. Esta norma pretendía también incluir la tipificación penal de la violación fundamentada en la ausencia de consentimiento. Sin embargo, países como Alemania y Francia se mostraron contrarios a este modelo, no alcanzándose acuerdo al respecto, dado que estos países no querían asumir el modelo que ya existe en España.

---

153 UE. COMISIÓN EUROPEA. *Código de Conducta para la lucha contra la incitación ilegal al odio en Internet*, 2020. Disponible en: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=42855

154 UE. 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. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80770

155 La transposición es el proceso por el que se incorporan las directivas de la Unión Europea (UE) a las legislaciones nacionales de los Estados miembros de la UE. Es la adaptación de la normativa interna de cada Estado para alcanzar los objetivos recogidos en la directiva.

También, en relación con la parte penal, se produce una importante referencia a las situaciones de ciberviolencia o violencia de género en línea, ya que se recoge la necesidad de establecer definiciones armonizadas de los delitos y las sanciones relacionados con determinadas formas de violencia en las que la acción delictiva está intrínsecamente vinculada al uso de las tecnologías de la información y de la comunicación, lo que deriva en la amplificación de los efectos perjudiciales del delito. Además, recoge expresamente que la ciberviolencia puede tener el efecto de silenciar a las mujeres y obstaculizar su participación social. Y reconoce que, en entornos educativos, escuelas y universidades, afecta desproporcionadamente a mujeres y niñas, siendo causa de exclusión social y ansiedad, llegando en ocasiones a provocar situaciones de autolesión en supuestos extremos.

Junto a ello, la nueva regulación incita a los Estados miembros a que se asesoren y colaboren con los servicios especializados para mujeres con el fin de elaborar y revisar las directrices para las autoridades encargadas de la persecución del delito con el objetivo de instaurar mejores prácticas. A su vez, se debe ofrecer a las víctimas de las diversas formas de ciberviolencia servicios de apoyo especializados. Además, establece el derecho a recibir información sobre cómo documentar el ciberdelito y sobre los recursos judiciales disponibles y mecanismos de eliminación de contenidos en línea relacionados. En cuanto a la supresión de contenidos, los Estados miembros deben fomentar la cooperación en materia de autorregulación entre los prestadores de servicios intermediarios.

En cuanto a los ciberdelitos de género, la normativa europea refuerza la protección y la lucha contra el ciberacoso, mayoritariamente inflingido contra las mujeres y las niñas, al determinar que los países de la Unión Europea estarán obligados a criminalizar el ciberacoso, el ciberacecho, la incitación al odio o la violencia a través de Internet y el compartir imágenes íntimas de modo no consensuado. También exige la sanción del envío mediante la tecnología de material que represente los genitales de una persona cuando provoque daños psicológicos, así como el hacer público por medio de mecanismos electrónicos, material que contenga datos personales sin consentimiento, con el fin de incitar a terceros a causar lesiones físicas o psicológicas graves a la víctima.

Como es habitual también en las Directivas de contenido penal, se establece una lista de circunstancias agravantes para estos delitos que deberán acatar todos los Estados miembros, entre ellas: cometer el crimen contra menores o en presencia de ellos, en el seno de la familia, matrimonio o convivencia, abusando de una posición de poder, o sobre personas con discapacidad, periodistas o defensoras de derechos humanos. Algunas de estas conductas, en el caso de España, ya se encuentran contempladas en el Código Penal.

Sin embargo, y como ya se ha dicho, a pesar de que una parte importante de la Directiva se refiere a la ciberviolencia de género, no concede una definición de violencia sino que se limita a proporcionar ejemplos de acciones que pueden ser calificadas como tal, aunque en el texto proyectado sí que recogía, en su artículo 4, una definición: *«todo acto de violencia cometido, asistido o agravado en parte o en su totalidad mediante el uso de las tecnologías de la información y de las comunicaciones».*

La tipificación propuesta de los delitos resulta algo confusa, ya que sólo se refiere al castigo del acecho y del acoso cuando se materializan a través de la tecnología. Penalizar únicamente tales actos cuando se realizan utilizando la informática deja fuera del castigo conductas que también lesionan los mismos

bienes jurídicos. Por ello, con independencia de que los requisitos puedan ser diferentes en el ámbito analógico que, en el digital, no debe dejar de sancionarse el acoso cuando vaya más allá de la mera molestia, como ocurre en nuestro ordenamiento jurídico en el artículo 172 ter, por lo que simplemente habrá que revisar para la transposición si, efectivamente, es necesario incluir alguna de las agravantes o si hay que diferenciar, necesariamente, entre acoso y acecho.

Igualmente, la Directiva 2024/1385 tampoco establece el acoso laboral como forma de violencia contra las mujeres, conforme ya se resaltaba en el Dictamen del Comité Económico y Social Europeo *Lucha contra la violencia contra las mujeres* a la Propuesta de Directiva en 2022. En este sentido, en el Estudio sobre el Impacto de la Propuesta de Directiva sobre violencia contra las mujeres, el Lobby Europeo de Mujeres en España, así como otras organizaciones de mujeres, entre ellas la Asociación de Mujeres Juristas Themis, señalaban que dentro del acoso laboral se debería incluir cualquier forma de acoso por razón de género (discriminaciones en procesos de contratación, los cambios de puesto de trabajo o el despido). La reciente Directiva aprobada sólo recoge el acoso sexual en el trabajo. Por otra parte, este estudio del Lobby Europeo de Mujeres en España puntualizaba que penalizar la difusión no consentida de material íntimo o manipulado, el ciberacecho y el ciberacoso exclusivamente cuando se comentan con el uso de las nuevas tecnologías deja fuera todas aquellas conductas que se comentan por otro medio que pudieran tener el mismo impacto, como pueden ser las copias en papel o buzoneándolas.

Asimismo, en la redacción final de la Directiva europea 2024/1385 parece que la violencia de género dentro de las relaciones de pareja o expareja ha quedado difuminada, siendo incluida dentro de la definición de violencia doméstica, ya que en esta no existe una carga histórica de dominación y creencia de poder del hombre sobre la mujer[156].

2.8. *Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual*

Conocido como *Convenio de Lanzarote*, es un tratado internacional adoptado por el Consejo de Europa en 2007, cuyo objetivo es proteger a los niños contra la explotación sexual y el abuso sexual. Este Convenio establece medidas integrales para prevenir estos tipos de violencia, identificar situaciones de riesgo y proteger a las víctimas.

El Convenio de Lanzarote obliga a los Estados parte a tomar diferentes medidas para prevenir y combatir la explotación sexual y el abuso sexual de niños como, por ejemplo, la creación de organismos especializados, la implementación de programas de educación y sensibilización, la cooperación entre diferentes sectores (gobierno, sociedad civil, sector privado), entre otras.

---

[156] UE. Directiva (UE) 2024/1385 del PARLAMENTO EUROPEO y del CONSEJO, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, 2024. Vid., artículo 2 b), donde se define la violencia a doméstica como:

> «b) «*violencia doméstica*»*: todo acto de violencia de naturaleza física, sexual, psicológica o económica que se produzca dentro de la unidad familiar o doméstica, sean cuales sean los vínculos familiares biológicos o jurídicos, o entre cónyuges o excónyuges o parejas o exparejas, independientemente de que el autor del delito comparta o haya compartido el mismo domicilio con la víctima*».

Por otra parte, el Convenio establece mecanismos de cooperación internacional, intercambio de información y asistencia entre los Estados parte, con el fin de fortalecer la lucha contra la explotación sexual y el abuso sexual de niños a nivel internacional. Es un instrumento legal que busca proteger a las personas menores contra la explotación sexual y el abuso sexual, estableciendo medidas preventivas, de protección y de colaboración entre los Estados parte para garantizar su bienestar en todo momento.

El *«Comité de Lanzarote»*, es decir, el Comité de las Partes del Convenio, es el organismo creado para garantizar la implementación efectiva del Convenio de Lanzarote por los Estados parte. También se encarga de identificar buenas prácticas, en particular, durante las actividades de desarrollo de capacidades (visitas de estudio, conferencias, etcétera). Está compuesto por representantes de las 48 partes de la Convención (los miembros), así como por participantes y observadores que se reúnen periódicamente en sesiones plenarias, el Comité evalúa la situación de la protección de los niños contra la violencia sexual a nivel nacional sobre la base de la información proporcionada por las autoridades nacionales y otras fuentes.

Con motivo de la 41ª sesión plenaria, el Comité de las Partes del Convenio adoptó su octavo informe de actividades, que abarca el período comprendido entre el 3 de febrero de 2023 y el 15 de febrero de 2024. Este Comité examinará un proyecto de opinión sobre la prescripción de los delitos sexuales contra niños y un proyecto de estudio sobre los mecanismos de recopilación de datos de puntos focales con el fin de observar y evaluar el fenómeno de la explotación y el abuso sexual infantil en el contexto de las tecnologías emergentes. También, el Comité de las Partes tomará decisiones sobre los próximos pasos de su trabajo de seguimiento en relación con la protección de los niños contra el abuso sexual en el círculo de confianza, y abordará los desafíos planteados por las imágenes y/o vídeos sexuales autogenerados por los niños. En esta temática, las cuestiones tecnológicas resultan esenciales, puesto que, como es sabido, la pornografía infantil, incluida la pornografía virtual, se nutre de infinidad de acciones que se llevan a cabo a través del medio tecnológico.

2.9. *Estrategia europea para la Igualdad de Género*

La Comisión Europea, en la comunicación al Parlamento Europeo, al Consejo, al Comité Económico y Social europeo y al Comité de las Regiones llamada *Una Unión de la igualdad: Estrategia para la Igualdad de Género 2020-2025*, establece los objetivos políticos y las acciones concretas para cubrir uno de los valores fundamentales de la Unión Europea, la igualdad de género. Uno de sus objetivos principales es conseguir una Europa igualitaria desde el punto de vista de género, en la que la violencia de género, la discriminación sexual y las desigualdades estructurales entre mujeres y hombres sean cosa del pasado.

Las metas primordiales incluyen acabar con la violencia de género, luchar contra los estereotipos de género, cerrar las brechas de género en el mercado laboral, lograr la igualdad de participación en diversos sectores económicos, abordar desigualdades salariales y de pensiones entre hombres y mujeres, reducir las diferencias en responsabilidades domésticas y lograr la paridad de género en la toma de decisiones y la actividad política. La Estrategia se basa en una combinación de integración de la perspectiva de género con acciones específicas, apoyada en el principio de interseccionalidad.

Aunque se enfoca en la UE, la Estrategia también se alinea con la política exterior de la UE en materia de igualdad de género y empoderamiento de las mujeres.

Además, incide en que la violencia en línea dirigida a las mujeres ha proliferado, con consecuencias concretas alarmantes, que supone un obstáculo a la participación de las mujeres en la vida pública. El acoso, la intimidación y los insultos en las redes sociales tienen repercusiones profundas en la vida cotidiana de las mujeres y las niñas[157].

La Comisión Europea en materia de igualdad propondrá la norma de servicios digitales para esclarecer las responsabilidades de las plataformas en línea con respecto a los contenidos difundidos por los usuarios. La norma de servicios digitales aclarará qué medidas se espera que apliquen las plataformas a la hora de atajar las actividades ilícitas en línea, al tiempo que protegen los derechos fundamentales. Los usuarios también tienen que ser capaces de actuar ante otros tipos de contenidos abusivos y nocivos, que no siempre se consideran ilícitos, pero que pueden tener consecuencias devastadoras. Con objeto de proteger la seguridad en línea de las mujeres, la Comisión facilitará el desarrollo de un nuevo marco de cooperación entre las plataformas de internet[158].

El 2022 fue el tercer año de implementación de la Estrategia y de adopción de medidas históricas para mejorar los derechos de las mujeres y la igualdad de género. Así, el 16 de noviembre entró en vigor la Ley de Servicios Digitales (DSA), que contiene obligaciones para evitar y prevenir la violencia digital contra las mujeres. Y, el 8 de marzo, la Comisión Europea adoptó una nueva propuesta de Directiva a escala de la Unión Europea para combatir la violencia contra las mujeres y la violencia doméstica, que introdujo normas mínimas específicas sobre los derechos de estas víctimas de delitos sin tipificar como era la ciberviolencia. Asimismo, el 22 de noviembre se adoptó la Directiva sobre equilibrio de género en los consejos de administración, cuyo objetivo fue lograr un mayor equilibrio de género en los puestos de toma de decisiones de las grandes sociedades de la Unión con cotización bursátil.

3. POLÍTICAS PÚBLICAS, LEYES Y NORMATIVA EN ESPAÑA.

3.1. *Normativa en materia de violencia de género tecnológica*

Fundamentalmente en materia de violencia de género digital, nuestro país se inspiró en la regulación europea, especialmente en los citados convenios de Budapest y Estambul. Y tomó como referencia ya citada Directiva 2013/40 del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información. La reforma del Código Penal de 2015, impulsada por esta Directiva, introdujo artículos fundamentales para la tipificación de los diversos tipos de cibercrimen, como el acceso no autorizado a sistemas informáticos (artículo 197 bis) o la penalización de la

---

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

158 Partiendo de la cooperación en el marco del Foro de la UE sobre Internet, que dio lugar a la adopción del Código de conducta de la UE para luchar contra la incitación ilegal al odio en línea.

producción, adquisición, importación o entrega a terceros de datos de acceso o software desarrollado o adaptado con el fin de cometer delitos (artículo 197 ter).

Es importante destacar que la criminalidad que se lleva a cabo a través de las tecnologías, antes conocida como criminalidad informática, y más tarde como ciberdelincuencia[159], no constituye una categoría delictiva autónoma en el sentido técnico jurídico y ello porque a través de la misma no se atenta, en la inmensa mayoría de los casos, contra bienes jurídicos nuevos, sino que los objetos de lesión o puesta en peligro existían antes de su aparición. Así, entre otros, el patrimonio, la intimidad, la libertad e indemnidad sexual y la integridad moral[160].

La ciberdelincuencia es un fenómeno criminal extraordinariamente vivo y en constante evolución, cuyas consecuencias afectan a toda la sociedad. Por ello obliga al legislador a buscar constantemente soluciones a las nuevas situaciones que se van generando como consecuencia del propio desarrollo tecnológico, adaptando la normativa a la realidad social en la que nos encontramos. En España estamos bien equipados para enfrentar esta forma de delincuencia, con una Estrategia de Ciberseguridad Nacional que aborda la seguridad cibernética como un problema que afecta a todas las áreas de la actividad humana, y que pretende garantizar un uso seguro y conveniente de las redes y los sistemas de información a través del refuerzo de la prevención, detección y adecuada contestación a los ciberataques.

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. A continuación, se van a ver 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 traspone la Decisión Marco 2004/68/JAI del Consejo de la Unión Europea en la tipificación de 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*», establece que aquel que, a través de Internet, teléfono u otra tecnología de la información y la comunicación, contacte a un 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.

---

159 MIRÓ LLINARES, F.; «El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio», Madrid, Marcial Pons, 2012, pp. 25.

160 Ibidem. Vid., pp. 28-29, en palabras de MIRÓ LLINARES, P.;
«la cibercriminalidad es hoy toda la criminalidad cometida en el nuevo espacio, al igual que la delincuencia tradicional es toda la ejecutada en el viejo. Es el lugar, en este caso, "el no lugar", el que define y marca los eventos sociales en él realizados y el que, por tanto, configura también como distinta la delincuencia en él ejecutada».

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, en 2015, se dictan dos normas: 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, 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, destinado a sancionar al que a través de medios tecnológicos contacte con un 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 CP, el antiguo artículo 183 bis CP, introducido por la LO 5/2010. Ambas regulaciones son, a todas luces, similares, por cuanto la reforma del año 2015 ha conservado, en gran parte, el articulado original.

Las modificaciones más significativas que trajo consigo la reforma de la Ley Orgánica 1/2015 incluyeron el aumento de la edad del sujeto pasivo de 13 a 16 años. Además, se 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, que exigía a España como Estado parte que incriminase tal delito de *acoso o hostigamiento o stalking.* Este nuevo tipo penal está destinado a ofrecer respuesta a conductas de gravedad incuestionable que, en numerosas ocasiones, no podían ser calificados como coacciones o amenazas. 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 un nuevo apartado, el número 8, al artículo 189 del Código Penal. Este apartado 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.

Además, se permite bloquear el acceso a estos sitios para los usuarios de Internet que se encuentren en España. Estas acciones pueden ser solicitadas de manera cautelar por el Ministerio Fiscal, con el fin de salvaguardar a los menores y a las personas con discapacidad en situaciones vulnerables.

En otro orden de cosas, la reforma establecida por la Ley 13/2015 adaptó en nuestro país gran parte de los delitos contemplados en el Convenio de Budapest, basándose en la Directiva 2013/40. Esta reforma 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 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 2021 no hay ninguna modificación sustantiva, año en el que se aprueba Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia. 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 se agrava la pena 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, en 2022 y en 2023, es preciso mencionar nuevas legislaciones. La Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la Libertad Sexual (LOGILS), cuyo objetivo es garantizar y proteger el derecho a la libertad sexual y su erradicación. Y, en este sentido, también abarca la violencia digital. 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 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. Como anticipa LLORIA GARCÍA[161], *«El espíritu de la norma, aunque está mal redactado [artículo], es que a los terceros se les castigue»,* aunque *«eso es lo que quiere castigar, no se sabe si se va a conseguir, por la reciente interpretación que hizo el Tribunal Supremo en la Sentencia núm. 699/2022, de 11 de julio, sobre qué es obtener y qué es recibir*» comportamientos que, hasta la fecha de la reforma, únicamente eran perseguidos en la vía civil por perjudicar el derecho al honor, a la intimidad personal y familiar y/o a la propia imagen de la víctima. Por tanto, se trata de 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.

Por último, 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.

3.2. *Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales*

En junio de 2024, el Consejo de Ministros ha aprobado el Anteproyecto de Ley Orgánica para la protección de menores en el entorno digital, que estará acompañado de una estrategia nacional para armonizar la normativa en el ámbito europeo. Este Anteproyecto se apoya en varias líneas estratégicas, como la prevención y formación en competencias digitales para los y las menores, las familias y los profesionales, la modificación del Código Penal para abordar delitos en entornos digitales, garantía de derechos de intimidad, honor e integridad de los menores, y refuerzo de la protección con mecanismos de control parental y verificación de edad en páginas *web*.

---

[161] LLORIA GARCÍA, P.; «Por qué la difusión de imágenes sexuales en plataformas online sin el consentimiento de las personas que aparecen en ellas es delito» Maldita.es, 20 de junio de 2022. Disponible en: https://maldita.es/malditatecnologia/20220620/difusion-imagenes-sexuales-plataformas-online-delito/

En el texto destacan medidas como la creación de espacios de encuentro para actividades fuera del ámbito digital en un ambiente saludable, la investigación de los efectos del consumo de pornografía en edades tempranas y la articulación de medidas para impedir los riesgos asociados al consumo de este contenido adulto. Para ello, entre otras acciones, se pretende elevar la edad para prestar el consentimiento al tratamiento de datos de carácter personal de 14 a 16 años, así como ampliar los supuestos en los que se podrá interrumpir judicialmente la prestación de servicios *online* o la retirada de datos.

Dentro del ámbito sanitario, la norma enfatiza la detección precoz de patologías relacionadas con el empleo de tecnologías digitales y la creación de centros especializados para enfrentar esas patologías.

En el sector docente, impulsar la educación en ciudadanía digital, la alfabetización digital, y la formación en el respecto a la privacidad, la propiedad intelectual, la protección de datos y los riesgos que se derivan de las redes sociales.

En la parte jurídica, 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[162]. 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.

Junto a ello se incluyen sanciones para los adultos 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.

También 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. Igualmente, 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.

Además, 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.

---

[162] En el texto proyectado, según el texto que se ha proporcionado por el Ministerio para alegaciones públicas, el art. 173 bis quedaría redactado del siguiente modo:

> «Se impondrá la pena de prisión de uno a dos años a quienes, sin autorización de la persona afectada y con ánimo de menoscabar su integridad moral, difundan, exhiban o cedan su imagen corporal o audio de voz generada, modificada o recreada mediante sistemas automatizados, software, algoritmos, inteligencia artificial o cualquier otra tecnología, de modo que parezca real, simulando situaciones de contenido sexual o gravemente vejatorias. Se aplicará la pena en su mitad superior si dicho material ultrafalsificado se difunde a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías, de modo que aquel se hiciera accesible a un elevado número de personas en el espacio virtual».

4. POLÍTICAS PÚBLICAS, LEYES Y NORMATIVA AUTONÓMICA

Varias comunidades autónomas españolas han puesto en funcionamiento normativa, protocolos y mecanismos de protección o reconocimiento de la ciberviolencia. Algunas de estas comunidades son:

1. Andalucía. En su Ley 7/2018, de 30 de julio, por la que se modifica la Ley 13/2007, de 26 de noviembre, de medidas de prevención y protección integral contra la violencia de género[163], recoge expresamente la violencia de género digital en su artículo 3.4.m):

> «*La ciberviolencia contra las mujeres es aquella violencia de género en la que se utilizan las redes sociales y las tecnologías de la información como medio para ejercer daño o dominio, entre las que figuran el ciberacoso, ciberamenazas, ciberdifamación, la pornografía no consentida, los insultos y el acoso por motivos de género, la extorsión sexual, la difusión de imágenes de la víctima y las amenazas de violación y de muerte*».

Asimismo, el Instituto Andaluz de la Mujer impulsa el *Protocolo de detección e intervención en la atención a víctimas de ciberdelincuencia de género*, con el fin de ofrecer a sus profesionales los instrumentos y las directrices necesarias para atender de manera idónea a las víctimas que acuden a su red y que presentan síntomas de sufrir violencia de género a través de las redes sociales. El Protocolo incluye la identificación y recopilación de información en sus formularios de atención (psicológica, jurídica y social), la evaluación de la situación, el diagnóstico correspondiente y la planificación de la intervención en materia de seguridad informática. Esto se realiza en coordinación con el área legal para tomar las medidas necesarias, así como la implementación de estrategias psicológicas para ayudar a las víctimas a sobrellevar los efectos de la exposición a pruebas electrónicas durante el proceso judicial.

El Plan Estratégico para la Igualdad de Mujeres y Hombres en Andalucía 2022-2028 destaca la importancia de las TIC en la actualidad y la necesidad de garantizar la igualdad en ese ámbito. En concreto, cada administración pública andaluza será responsable de llevar a cabo un análisis detallado del estado de situación de mujeres y hombres en su ámbito de competencia para diseñar los planes de igualdad correspondientes. Este diagnóstico permitirá establecer objetivos de mejora y justificar las medidas propuestas en el Plan. Además, sugiere ampliar el enfoque para incluir datos sobre posibles desigualdades relacionadas con la presencia desigual de mujeres y hombres en sectores económicos emergentes, como el de las TIC (en su vertiente empleo o economía de empresa), el uso diferenciado del ocio y la calidad de vida, la salud mental, la violencia en las redes sociales, el ciberacoso y los nuevos tipos de violencia machista, y la percepción social sobre la desigualdad, entre otros aspectos. Esta idea se consolida y hereda del plan estratégico andaluz de 2010-2013, que indicaba que para atender esas necesidades los y las profesionales necesitan, a su vez, nuevos conocimientos, herramientas y pautas sobre TIC, redes sociales y ciberdelincuencia de género.

---

[163] BOE. Ley 7/2018, de 30 de julio, por la que se modifica la Ley 13/2007, de 26 de noviembre, de medidas de prevención y protección integral contra la violencia de género. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-11883

2. Castilla-La Mancha. En su Ley 4/2018, de octubre, para una Sociedad Libre de Violencia de Género[164] recoge la ciberviolencia contra las mujeres en su artículo 4 apartado h):

> «*Las manifestaciones de violencia ejercida a través del uso de las tecnologías y de los medios sociales: cualquier lesión de la dignidad, integridad, intimidad y libertad de las mujeres que se produce a través de tecnologías de la información y la comunicación, ya sea a través del acoso, la extorsión, la divulgación de imágenes privadas o cualquier otra conducta que banalice, justifique o aliente la violencia hacia las mujeres, incluyendo la que se produce en las primeras relaciones afectivas entre jóvenes adolescentes*».

3. Cataluña. La Ley 17/2020, de 22 de diciembre, de modificación de la Ley 5/2008, del derecho de las mujeres a erradicar la violencia machista en su artículo 4, apartado f) hace referencia a la violencia digital:

> *«Violencia digital: consiste en aquellos actos de violencia machista y misoginia en línea cometidos, instigados, amplificados o agravados, en parte o totalmente, mediante el uso de tecnologías de la información y de la comunicación, plataformas de redes sociales, webs o foros, correo electrónico y sistemas de mensajería instantánea y otros medios similares que afecten a la dignidad y los derechos de las mujeres. Estos actos causan daños psicológicos e incluso físicos; refuerzan estereotipos; dañan la dignidad y la reputación; atentan contra la privacidad y libertad de obrar de la mujer; le causan pérdidas económicas, y plantean obstáculos a su participación política y a su libertad de expresión».*

Y, en su artículo 8 bis, menciona la investigación en la violencia machista digital:

> «*La investigación en violencia machista digital debe orientarse a la tipología de mujeres que reciben esta violencia, el tipo de la violencia que reciben, su frecuencia, el tipo de perfiles que la protagonizan y que divulgan estos discursos, las plataformas donde los abusos y la violencia tienen lugar, el impacto de esta violencia individualmente y en cuanto a los derechos fundamentales de las mujeres y a los derechos humanos, la respuesta policial y judicial, el índice de denuncias efectivamente presentadas respecto al número de las que podrían y deberían haberse presentado, y las causas por las que no se llegan a presentar o son archivadas, el impacto en las personas que denuncian la violencia ejercida hacia la mujer y la respuesta institucional de protección de estas personas».*

3. Galicia. En la Ley 15/2021, de 3 de diciembre, por la que se modifica la Ley 11/2007, de 27 de julio, gallega para la prevención y el tratamiento integral de la violencia de género, en el artículo 3 h) conceptualiza la violencia de género digital o violencia en línea contra la mujer:

> «*que incluye todo acto o conducta de violencia de género cometido, instigado o agravado, en parte o en su totalidad, por el uso de las nuevas tecnologías de la información y la comunicación (TIC), como Internet, plataformas de redes sociales, sistemas de mensajería y correo electrónico o servicios de geolocalización, con la finalidad de discriminar, humillar, chantajear, acosar o ejercer dominio, control o intromisión sin consentimiento en la privacidad de la víctima; con independencia de que el agresor guarde o no relación conyugal, de pareja o análoga de afectividad en el presente o en el pasado, o de parentesco con la víctima.*

---

[164] BOE. Ley 4/2018, de 8 de octubre, para una Sociedad Libre de Violencia de Género en Castilla-La Mancha. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2018-17065

Igualmente, tendrán la consideración de actos de violencia digital contra la mujer los ejercidos por hombres de su entorno familiar, social, profesional o académico.

Se exceptúan las herramientas de control parental que cumplan con la legislación vigente destinadas a la protección y seguridad de las personas menores de edad».

4. La Rioja. En la Ley 11/2022, de 20 de septiembre, contra la Violencia de Género de La Rioja[165] se incluye la violencia digital o ciberviolencia dentro de las formas y manifestaciones de violencia de género en su artículo 5 apartado j), describiéndola como,

> *«toda conducta o acto violento contra las mujeres, llevado a cabo a través de las tecnologías de la información y la comunicación*».

5. Madrid. El Plan de Ciberseguridad para la Ciberprotección y por la Convivencia 2023-2027 pretende la implementación de estrategias que mejoren la prevención, en materia de ciberacoso dirigida a estudiantes de 4º, 5º y 6º de Educación Primaria, Educación Secundaria Obligatoria y profesores y familias. Se trata de advertir al alumnado acerca de los riesgos de Internet como el *sexting* (envío de imágenes y vídeos de carácter sexual), *grooming* (acoso sexual a menores), acceso a la pornografía o el contacto con foros que entrañan riesgos y fomentan hábitos como la anorexia, la bulimia, autolesión o discursos de odio.

5. DELITOS RELACIONADOS CON LA TECNOLOGÍA EN EL CÓDIGO PENAL ESPAÑOL

Como consecuencia de la propagación del uso de Internet y las nuevas tecnologías para la comisión de conductas con fines sexuales, nuestro Código Penal impulsa diferentes reformas, que pasamos a exponer en materia de ciberviolencia o violencia digital de género.

5.1. Grooming *o ciberacoso sexual a menores*

Según nuestro Alto Tribunal, en la sentencia núm. 174/2017, de 21 de marzo, el denominado *«child grooming»* es:

> *«el término de origen inglés se refiere a la acción deliberada de un adulto que pretende acosar y/o abusar sexualmente de un niño/a adolescente a través de Internet. Para conseguir su finalidad, los 'groomers' crean perfiles falsos en redes sociales u otras plataformas de chat similares inventándose una vida o persona que no son. Además de entablar conversaciones por tiempos prolongados, el propósito del diálogo es establecer confianza y pedir al menor contenido sexualmente explícito. Las fotos y vídeos eróticos son el principal medio de acción del 'Grooming', este primer paso puede producir un encuentro físico, lo que desenlaza en un acoso moral, o algo peor como una violación o un asesinato. Asimismo, una vez que la víctima decide compartir*

[165] BOE. Ley 11/2022, de 20 de septiembre, contra la Violencia de Género de La Rioja. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2022-16127

material a través de engaños, el 'groomer' comienza a chantajear al menor, amenazándolo con publicar sus fotos y vídeos si no entrega más o se niega a un encuentro personal».

El artículo 183 del CP castiga, con la pena de prisión de uno a tres años o multa de doce a veinticuatro meses, las conductas consistentes en contactar con un menor de 16 años realizadas con el soporte de las nuevas tecnologías, Internet, teléfono o cualquier otra tecnología de la información, por una persona adulta o menor de edad y encaminada a ganarse su confianza, con el objetivo de concertar un encuentro a fin de cometer posteriormente otro delito contra la libertad sexual de los contemplados en los artículos 181 y 189 del Código Penal (delito de agresión sexual y/o pornografía contra menores) para los que se impondrán las penas que correspondan por cada uno de ellos.

Dado que nuestro CP autoriza el castigo como agresión sexual de los autocontactos en el caso de menores, el encuentro puede ser analógico, pero también tendrán cabida en los delitos de agresión sexual los encuentros virtuales, por lo que también se debería castigar en concurso[166].

El delito se comete en el momento en que se contacta con un menor mediante actos encaminados al acercamiento con el fin de cometer un delito posterior contra la indemnidad sexual, no siendo necesario que se realice esta última conducta. A pesar de que se le conoce como ciberacoso, la jurisprudencia coincide en que basta con un sólo contacto para cometer el delito. Por lo tanto, no es necesario que exista un acoso constante o una comunicación continuada.

En este mismo artículo 183 se contempla una circunstancia agravante. Cuando el acercamiento se produzca con intimidación, engaño o coacción, se aplicará la pena en su mitad superior.

También se contempla un tipo atenuado, que castiga con la pena de prisión de seis meses a dos años en el artículo 183.2 del Código Penal a quien embauque a un menor usando medios tecnológicos o telemáticos, con el fin de que este le facilite material pornográfico o le muestre imágenes pornográficas en las que se represente o aparezca un menor. El tipo solamente exige el contacto con el menor a través de teléfono o cualquier otro medio tecnológico encaminado al embaucamiento.

En relación con estas conductas, el Código Penal contiene una causa de atipicidad, que elimina la presunción de invalidez del consentimiento para el supuesto en que exista consentimiento de la víctima menor de 16 años y el autor sea una persona próxima al menor por edad y grado de desarrollo o madurez física y psicológica (art. 183 bis CP). Esta exención no sería aplicable cuando se utilice violencia, intimidación o abuso de una situación de superioridad o de vulnerabilidad de la víctima, así como cuando los actos se ejecuten sobre personas que se hallen privadas de sentido o de cuya situación mental se abusare y los que se realicen cuando la víctima tenga anulada por cualquier causa su voluntad (art. 178.2 CP).

Este delito habitualmente es cometido por una persona adulta, aunque no excluye que el sujeto activo pueda ser una persona menor de edad. En todo caso, el desarrollo de la acción comienza con una

---

166 LLORIA GARCÍA, P.; «El delito de Child grooming y el consentimiento de menores de 16 años (arts. 183 y 183 bis del CP)», en MARTINEZ GALINDO, G., MAESTRE DELGADO, E.; «La reforma de los delitos sexuales», J.M Bosch, Madrid, 2024, pp. 201-234.
Vid.; STS núm. 97/2015, Sala 2ª, de lo Penal, de 24 de febrero, Rec. 1774/2014.

primera actividad, que consiste en la creación de un perfil falso en redes sociales o foros de Internet frecuentado por menores, simulando ser también una persona menor de edad. Para ello, se aportan imágenes (fotografías o vídeos) para acercarse sin reservas a la posible víctima. Tras el acercamiento, se consiguen datos privados de la víctima como su dirección, el colegio al que asiste, los lugares de ocio que frecuenta, etc. El autor suele dar un paso más allá cuando ya tiene los datos personales del o la menor. Ese es el momento en que le solicita material comprometedor, como fotografías o vídeos. Una vez que el adulto tiene en su poder este material, emplaza al menor a concertar una cita con la intención de cometer ese segundo delito al que hemos hecho referencia. Cuando el menor o la menor se oponen, surgen las coacciones o amenazas de publicar el material de que dispone.

En ocasiones, el acercamiento es virtual y el encuentro también, consiguiendo que el o la menor lleven a cabo prácticas sexuales consigo mismo o con otras personas menores, o desnudos con connotaciones pornográficas ante la cámara, lo que se aprovecha para grabar esas imágenes y comenzar así la ciberextorsión.

La Sala de lo Penal del Tribunal Supremo se ha pronunciado en numerosas sentencias, en las que se pone de manifiesto el *modus operandi* en esta tipología delictiva. Entre otras, destacan dos sentencias: la primera, la Sentencia núm. 447/2021, Sala 2ª, de lo Penal, de 26 de mayo, Rec. 3097/2019, que aborda un supuesto de intimidación y amenazas a una menor a través de las redes sociales para que envíe fotos o vídeos de ella de contenido sexual. Se le advierte de que, de negarse, se publicarán otros archivos de similar contenido que se han obtenido mediante engaño. La condena es por una agresión sexual y un delito de corrupción de menores. El Tribunal determina que la distancia física entre el agresor y la víctima no desnaturaliza la agresión sexual, ya que la intimidación atenta contra la libertad sexual de la víctima en un escenario con impacto nocivo y duradero como es Internet. La sentencia destaca la especial vulnerabilidad de la víctima y la importancia de protegerla. Es una sentencia relevante, ya que entiende que se produjo la agresión sexual, aunque no hubo un contacto físico y establece que la ciberintimidación puede ser suficiente para integrar el concepto de intimidación propio de los delitos de agresión sexual violentos. Y, la segunda resolución, es la Sentencia núm. 376/2023, Sala 2ª, de lo Penal, de 18 de mayo, Rec. 10566/2022, que condena por múltiples delitos de ciberacoso sexual infantil, exhibicionismo, abuso sexual y elaboración de pornografía infantil. En los hechos probados se incluye el contacto con menores a través de redes sociales, el envío de material sexual explícito, la coerción para obtener imágenes y vídeos de contenido sexual a menores, así como la propuesta de mantener relaciones sexuales. La resolución enfatiza la importancia de la interacción digital como forma de acercamiento en delitos contra menores. También remarca la condición de profesor del acusado a la hora de fijar la pena. Lo importante de esta resolución radica, por un lado, en la idea de que la ciberintimidación es suficiente para integrar la intimidación necesaria para obtener un consentimiento inválido y, por otro, en que baste con los encuentros virtuales para entender consumado el delito de agresión sexual en el caso de menores.

5.2. Stalking *o acoso predatorio* (Ciberstalking)

La incorporación de este tipo delictivo en nuestro ordenamiento penal, como ya habíamos mencionado a lo largo del estudio se dirige a ofrecer respuesta a aquellas conductas de indudable gravedad que no podían ser calificadas como coacciones o amenazas. Se considera que existen actuaciones en las

que se llevan a cabo comportamientos de acoso persistente o intentos de comunicación frecuentes, que son suficientes para generar una inquietud y malestar relevantes desde el punto de vista penal. Estas conductas pueden ocasionar un grave deterioro en la libertad y en la sensación de seguridad de la víctima, sometiéndola a constantes persecuciones, vigilancias, llamadas repetidas u otros actos continuos de hostigamiento.

En su primer informe a España, de 13 de octubre de 2020, GREVIO destacó positivamente que España haya sido pionera en Europa al criminalizar de forma explícita el acoso perpetrado a través de tecnologías digitales, a pesar de que en el artículo 172 ter del CP no se recogía en ese momento ninguna referencia expresa al uso de la tecnología, o un incremento de pena en el caso de introducirse algún elemento tecnológico.

Como se ha señalado, el acoso u hostigamiento está regulado en el artículo 172 ter del Código Penal, que castiga, en su tipo básico, con la pena de prisión de 3 meses a dos años o multa de 6 a 24 meses, y presenta una estructura que puede sistematizarse en la exigencia de los siguientes elementos:

1. Acosar a una persona de forma insistente y reiterada.
2. Reiteración de conductas contenidas en el propio artículo:
   a) vigilar, perseguir o buscar cercanía física;
   b) intentar establecer comunicación por cualquier medio o a través de terceras personas;
   c) usar indebidamente sus datos personales para adquirir productos o mercancías, o contratar servicios, o conseguir que terceras personas se pongan en contacto y
   d) atentar contra su libertad o patrimonio o la libertad o patrimonio de personas próximas.
3. Un elemento negativo del tipo, consistente en la ausencia de legitimación para desarrollar dichas conductas.
4. Exigencia de la producción de un resultado, consistente en alterar con estos comportamientos el normal desarrollo de la vida cotidiana de la víctima.

Una de las primeras cuestiones que se plantean es si esa insistencia y reiteración se refieren o no a una sola de las conductas fijadas en el tipo. Este punto ha quedado solventado por la Sala 2ª, de lo Penal del Tribunal Supremo en Sentencia núm. 324/2017, de 8 de mayo, Rec. 1775/2016, que determina que los términos insistencia y reiteración deben ser utilizados de manera general, es decir, teniendo en cuenta cualquiera de las cuatro modalidades descritas en los numerales del 1 al 4. Así se refiere a ello:

> *«la reiteración de que habla el precepto es compatible con la combinación de distintas formas de acoso. La reiteración puede resultar de sumar acercamientos físicos con tentativas de contacto telefónico, por ejemplo, pero siempre que se trate de las acciones descritas en los cuatro apartados del precepto»*. Esta sentencia, en relación con la insistencia y reiteración y la falta de indicación en cuanto a la cantidad de veces que debe darse la intromisión para encajar en el tipo penal, indica que *«no sería sensato ni pertinente ni establecer un mínimo número de actos intrusivos como se ensaya en algunas definiciones, ni fijar un mínimo lapso temporal. Pero sí podemos destacar que el dato de una vocación de cierta perdurabilidad es exigencia del delito descrito en el artículo 172 ter del Código Penal, pues solo desde ahí se puede dar el salto a esa incidencia en la vida cotidiana».*

El Alto Tribunal en su STS núm. 554/2017, Sala 2ª, de lo Penal, de 12 de julio, Rec. 1745/2016 estudia el delito de *stalking* y resalta la aplicación del delito de acoso en el ámbito de las relaciones personales, enfatizando la necesidad de salvaguardar la libertad y la seguridad de las víctimas ante comportamientos intrusivos y repetitivos que pueden provocar miedo y perturbación en su vida diaria.

En definitiva, estas dos resoluciones del Tribunal Supremo definen el delito de *stalking* por diversas características clave: la actividad debe ser insistente, reiterada y permanente, superando lo molesto, y englobar diferentes formas de acoso, tanto acercamientos físicos como contactos telefónicos, y que el autor debe carecer de autorización para llevarlas a cabo. Además, debe afectar a los hábitos y rutinas de la víctima. Los tribunales consideran que el acoso debe ser un comportamiento continuo a lo largo del tiempo sin un periodo específico definido y con un marcado carácter intrusivo.

Otra cuestión controvertida ha sido ese requerimiento de un resultado, *«altere el normal desarrollo de su vida cotidiana»*. En relación con esta cuestión, la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual, se inclinó, acorde con las recomendaciones realizadas por el GREVIO[167] encaminadas a revisar el nivel de gravedad requerido para que una conducta sea calificada como acoso, puesto que en su informe manifestaba su preocupación ante considerar acoso solamente cuando altera significativamente la rutina diaria de la víctima, invirtiendo así la carga de la prueba al centrarse en las víctimas y no en los agresores y exigiendo un nivel de gravedad de la conducta muy elevado. A raíz de estas sugerencias, la reforma efectuada en 2022 pasó a sustituir la expresión «altere gravemente» por «altere el normal». Al tratarse de una reforma relativamente reciente, veremos cómo se aplica por los tribunales, ya que se trata de un concepto jurídico indeterminado.

En el mismo artículo 172 ter se recogen dos subtipos agravados, que atienden a la situación o condición de la víctima.

1. *«Cuando la víctima se halle en una situación de especial vulnerabilidad por razón de su edad, enfermedad, discapacidad o por cualquier otra circunstancia»,* la pena de prisión se eleva respecto del tipo básico de tres a seis meses, sin variación en el límite superior que se sitúa en dos años. Y, además, se elimina la posibilidad de condenar a pena de multa.
2. *«Cuando la víctima sea alguna de las que se refiere el apartado segundo del artículo 173»*[168], siendo la pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días.

---

[167] GREVIO. *Primer Informe de evaluación sobre las medidas legislativas y de otra índole que dan efecto a las disposiciones del Convenio del Consejo de Europa sobre Prevención y Lucha contra la violencia contra las Mujeres y la Violencia Doméstica (Convenio de Estambul) ESPAÑA*. Inf (2020)19. Disponible en: https://violenciagenero.igualdad.gob.es/marcoInternacional/informesGREVIO/docs/InformeGrevioEspana.pdf

[168] El artículo 173 del CP establece, en este sentido:
«quien sea o haya sido su cónyuge o sobre persona que esté o haya estado ligada a él por una análoga relación de afectividad aun sin convivencia, o sobre los descendientes, ascendientes o hermanos por naturaleza, adopción o afinidad, propios o del cónyuge o conviviente, o sobre los menores o personas con discapacidad necesitadas de especial protección que con él convivan o que se hallen sujetos a la potestad, tutela, curatela, acogimiento o guarda de hecho del cónyuge o conviviente, o sobre persona amparada en cualquier otra relación por la que se encuentre integrada en el núcleo de su convivencia familiar, así como sobre las personas que por su especial vulnerabilidad se encuentran sometidas a custodia o guarda en centros públicos o privados».

En este segundo supuesto, se señala que es habitual que, con posterioridad a la finalización de la relación sentimental, sean frecuentes los supuestos de hostigamiento incesante y grave contra la mujer, mediante el empleo de medios electrónicos: reiteración de llamadas telefónicas y/o mensajes en redes sociales y servicios de mensajería instantánea. Ello afecta a la vida normal de la víctima, quien queda sometida durante todo el tiempo que dure la conducta a una invasión e injerencia en su libertad y a un quebranto de la libre determinación de comportarse conforme a la propia voluntad. El legislador encuadra el delito de acoso/*ciberstalking* como un tipo de violencia de género, que permitirá a la víctima solicitar una medida de protección del artículo 544 ter de la Ley de Enjuiciamiento Criminal hasta la celebración del juicio, además de una agravación de la pena.

Como quiera que un proceso de ruptura también lleva consigo la necesidad de comentar y discutir diferentes cuestiones personales y patrimoniales entre los que han sido pareja, el problema radica en determinar el límite a partir del cual la reiteración de la comunicación deviene constitutiva de delito. A estos efectos, resulta gráfica la Sentencia de la Audiencia Provincial de Madrid núm. 313/14, Sección 27, de 22 de mayo, Rec. 779/2014, según la cual:

> «Claro que no es delictivo que una persona trate de comunicar con otra persona para discutir distintas cuestiones, incluso de modo insistente. Esto forma parte de la realidad cotidiana. El problema empieza cuando se quiere imponer a toda costa el deseo personal y se hace violentando hasta el extremo la libertad ajena, cuando a pesar de tener la perfecta y completa conciencia de que esa persona no quiere mantener ningún tipo de contacto se le impone, asfixiándola y limitándola en su libertad».

El estudio *La ciberviolencia de mujeres y niñas* (2022), del Instituto Europeo de la Igualdad de Género, matiza que el hostigamiento o ciberacoso conlleva la existencia de incidentes reiterados constitutivos o no de actos inocuos por separado, pero que combinados socavan la sensación de seguridad de la víctima y provocándole a su vez angustia, miedo o alarma. Entre tales actos pueden figurar: el envío de correos electrónicos, mensajes de texto (SMS) o instantáneos con contenido ofensivo, amenazador o amoroso; la publicación de comentarios ofensivos o insinuaciones inapropiadas u ofensivas en Internet; compartir fotografías o vídeos íntimos de la víctima a través de Internet o del teléfono móvil, persecuciones físicas o virtuales o instalación de *software* espía para conocer todos los movimientos de la víctima, entre otros. Para que se considere ciberhostigamiento, estos actos debe cometerlos la misma persona de manera reiterada.

Ambas agravantes específicas tienen su fundamento en el artículo 46 del Convenio de Estambul cuando dispone que:

> «Las Partes adoptarán las medidas legislativas o de otro tipo necesarias para que las circunstancias que se expresan a continuación, siempre que no sean de por sí elementos constitutivos del delito, de conformidad con las disposiciones aplicables de su derecho interno, puedan ser tomadas en consideración como circunstancias agravantes en el momento de la determinación de las penas correspondientes a los delitos previstos en el presente Convenio:

a) que el delito se haya cometido contra un cónyuge o pareja de hecho actual o antiguo, de conformidad con el derecho interno, por un miembro de la familia, una persona que conviva con la víctima o una persona que abuse de su autoridad;

(…)

c) que el delito se haya cometido contra una persona que se encuentre en situación de vulnerabilidad por la concurrencia de particulares circunstancias;

d) que el delito se haya cometido contra o en presencia de un menor».

Con la Ley Orgánica de garantía integral de la libertad sexual, se incorpora un nuevo apartado quinto en el artículo 172 ter, que penaliza la utilización de la imagen de una persona sin su consentimiento para realizar anuncios o abrir perfiles falsos en redes sociales, páginas de contactos o cualquier medio de difusión pública, provocándole a la misma una situación de hostigamiento o acoso. La condena es de prisión de tres meses a un año o multa de seis a doce meses.

Con esta nueva disposición se busca abarcar legalmente situaciones comunes en la realidad, que no podrían ser consideradas como delito de acoso según la interpretación literal del primer apartado, ya que suelen implicar una única acción: por ejemplo, la publicación de un anuncio que incluye imágenes y el número de teléfono de otra persona en un sitio web de contactos, provocando este único acto múltiples (insistentes y reiteradas) llamadas de terceros. También acciones como presentarse en las redes sociales usurpando la imagen y personalidad de la víctima, lanzando mensajes impropios que no hubiera emitido nunca la víctima, generando así un daño a su reputación digital.

Recientemente, 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, introduce una agravación en relación con este apartado quinto cuando la víctima sea menor o persona con discapacidad, en cuyo caso, se aplicará la pena en su mitad superior.

5.3. Sexting *y sextorsión*

El *sexting* es una práctica sexual bastante frecuente y, por supuesto, lícita. Deriva de la idea de compartir imágenes (estáticas o dinámicas) de contenido sexual de manera voluntaria y consentida entre personas que protagonizan dichas imágenes de manera individual o conjunta.

Ciertamente, esta actividad sexual, como todas las que implican confianza con aquel que se practican, supone desprenderse o permitir que el otro o los otros tomen conocimiento de una situación íntima. Pero, a diferencia de lo que supone la puesta en práctica de actos sexuales de una u otra naturaleza, que desde luego cualquiera de los participantes puede divulgar narrándolo, en el caso del *sexting* la persona que aparece en las imágenes se desprende o autoriza a otro/otros a disponer de un material de contenido íntimo altamente sensible que, de ser indebidamente utilizado, genera una grave lesión de la intimidad de la persona o personas que aparecen en el mismo, además de una afectación a la dignidad y la integridad moral, sobre todo si se trata de una mujer, dada la consideración que tiene la sexualidad en nuestra sociedad. Como es sabido, el hecho de difundir imágenes practicando

sexo o en actitud erótica de mujeres toma como base el mito de la mujer pasiva sexualmente, para avergonzarla, humillarla y agredirla, mientras que, en el imaginario patriarcal, si son de un hombre, este se empodera, ensalza y glorifica.

Precisamente, esta concepción es la que produce que, en determinadas situaciones, el sujeto que dispone de dicho material lo utilice para doblegar la voluntad de quien aparece en él, obligándole a hacer algo que no quiere, o no hacer algo que quiere, bajo la amenaza de difundir dichas imágenes, que posee con la autorización de la persona (si proceden del *sexting*), o habiéndolas obtenido de manera fraudulenta o ilegal (obteniendo las imágenes sin autorización, bien mediante situaciones de *hacking*, u obligando a la víctima a entregarlas mediante engaño, coacción u otra situación que determine la invalidez del consentimiento).

Los motivos que pueden llevar a esta difusión son variados: en ocasiones la amenaza proviene de la pareja o expareja, condicionando la publicación de imágenes a temas de familia o sexo, como, por ejemplo: la reconciliación, la solicitud de ver a los hijos o hijas, o la amenaza de una custodia compartida.

También es una conducta frecuente tras la ruptura de pareja. Se da, sobre todo, en casos de infidelidad o de separación, colgando fotos comprometidas de las víctimas en la red después de la ruptura como modo de venganza. Este comportamiento puede afectar seriamente a la víctima, por un lado, por la concurrencia de una quiebra de la privacidad, especialmente porque la difusión en redes sociales implica una pérdida de control sobre las imágenes y, por otra parte, un menoscabo psicológico por la humillación.

En todos estos casos, se habla de la existencia de «sextorsión», que es una forma de extorsión. Implica amenazar con difundir dichas imágenes íntimas, sin consentimiento, si no se cumplen las exigencias del que posee el material, que pueden consistir en cualquier petición: más fotos de naturaleza similar, reanudar la relación de pareja, o un precio por la no difusión[169].

En ambas situaciones (cuando se difunde con o sin amenaza previa y cuando se amenaza con difundir), se está en presencia de violencia de género digital si las víctimas son mujeres o niñas, y suele ser el paso previo a la comisión del delito de difusión no consentida de imágenes intimas, por lo que conviene clarificar todas estas situaciones y determinar cómo se produce su castigo penal.

5.3.1. Sexting y difusión no consentida de imágenes íntimas obtenidas con consentimiento

El delito de difusión inconsentida de imágenes íntimas fue introducido en el año 2015 en el CP, como en el marco de los delitos contra la intimidad. En concreto, en el artículo 197.7. La necesidad del castigo obedecía a que no era posible encuadrar estas conductas en los delitos de revelación de secretos, precisamente porque el hecho de autorizar a poseer la imagen (bien porque se daba permiso

[169] En ocasiones, también se habla de sextorsión en casos de chantaje a hombres que visitan páginas pornográficas o que mantienen relaciones fuera de la pareja, o que son clientes de prostitución. Sin embargo, estos casos no entrarían, en puridad, en los supuestos de violencia digital que ocupan este estudio.

para grabar o tomar la foto, o bien porque se enviaba por quien aparecía en la misma) impedía hablar de delito contra la intimidad, ya que se entendía que la persona que así actuaba se desprendía de la misma, dejando en manos del receptor el hecho de difundir o no, puesto que la intimidad es un bien jurídico disponible y supone la exigencia de preservarla. Junto a ello, el CP, en el artículo 197.1 y 3, sólo establecía el castigo para la obtención de soportes con contenido íntimo sin autorización del titular y protegidos debidamente.

Por ello, se estableció el castigo (una pena de prisión de tres meses a un año o multa de seis a doce meses) a quien, habiendo obtenido las imágenes con permiso de la persona o personas que aparecen en las mismas, difunda, revele o ceda (envíe o entregue) a terceros, imágenes (fotografías) o grabaciones audiovisuales (vídeos, *gifs*, etc.) de aquella, sin autorización para tal acto de prestación a tercero.

Para garantizar que se trata de imágenes íntimas, esto es, que no eran públicas, se incluyó una exigencia locativa (que las imágenes se hubieran obtenido en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros) y un requisito de cualificación del resultado: no cualquier afectación de la intimidad, sino sólo cuando la difusión produzca un grave menoscabo de la misma.

Por lo tanto, el hecho supone revelar imágenes de fotografías o vídeos (no de soportes de voz exclusivamente), que afecten a la intimidad (sexual, preferentemente), que se han obtenido con consentimiento, pero que se difunden, ceden o revelan sin permiso.

Varias cuestiones esenciales se plantean ya de estas indicaciones: por un lado, el deber de autoprotección de la víctima y la naturaleza de las imágenes para ser consideradas íntimas, y qué significa obtener, como medio de averiguar quién es el sujeto activo del delito y si se puede castigar o no la redifusión de las imágenes, cuando llegan a poder de un tercero distinto del que las obtuvo.

En cuanto al carácter íntimo de la imagen, se ha discutido si ha de tener una naturaleza estrictamente sexual o si puede ser erótica y si, por tanto, los meros desnudos tienen cabida en el delito.

En este sentido se han pronunciado, entre otras, la Sentencia del Tribunal Supremo núm. 70/2020, de 24 de febrero, donde cuestiona por la parte que se haya producido una grave afectación de la intimidad, puesto que la imagen es sólo un desnudo, lo que puede ser socialmente adecuado (por no tener un contenido sexual explícito) y, además, la persona que recibe la imagen ya ha compartido intimidad con la víctima (era su pareja que recibe la imagen por parte de otro hombre que tenía relaciones con la mujer), por lo que no se ve lesionado dicho bien jurídico. Igualmente se dice por la defensa que la víctima obvió su deber de autoprotección, por enviar la imagen y porque, además, no lo hizo mediante un acto privado (lo que equipara a una fotografía en papel) sino a través de una «red social» (el equivalente a un medio digital, aunque lo hiciera sólo a la persona de su confianza), lo que le lleva a perder el control sobre sus datos, por lo que focaliza la responsabilidad en la víctima[170].

[170] Pretende establecer una situación de autopuesta en peligro de la víctima, acogiéndose a la antigua tesis del despojo de la intimidad, alegando prácticamente una compensación de culpas y negando la lesión del bien jurídico, por no haber llevado a cabo deberes de autoprotección. Confunde la parte la autoprotección (que es deseable en cualquier circunstancia de la vida y que no es exigible ni adecuada en todo caso) y la autopuesta en peligro (que implica una falta de cuidado, que pone a la víctima como responsable de lo que le ha ocurrido y puede llevar a una compensación de culpas) absolutamente rechazable.

Por último, incide en que cuestiona que se cumplimente adecuadamente el delito a través del verbo «obtener», puesto que entiende que la imagen no la obtuvo el que después difundió, como señala el tipo, en el domicilio o en un lugar apartado de la vista de terceros, sino que se la mandó la propia víctima, vinculando la acción típica al lugar de realización de la imagen, e intentando diferenciar entre el verbo «obtener» y el verbo «recibir»[171]. A lo que el Tribunal contesta alegando que:

> «(…) La acción nuclear consiste en difundir imágenes "obtenidas" con el consentimiento de la víctima en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros. El vocablo "obtener" –según el diccionario de la RAE– es sinónimo de alcanzar, conseguir, lograr algo, tener, conservar y mantener. Resulta muy difícil sostener que cuando esas imágenes se remiten por la propia víctima y se alojan en el móvil del destinatario, en realidad, no se consiguen, no se logran, no se tienen, no se conservan o no se mantienen.
>
> (…) Tampoco puede identificarse la Sala con el argumento esgrimido por el recurrente –con algún apoyo dogmático– de que fue la propia víctima la que creó el riesgo de su difusión, remitiendo su propia foto al acusado a través de un programa de mensajería telemática. Ese razonamiento, llevado a sus últimas consecuencias, puede llegar a justificar la lesión en bienes jurídicos del máximo valor axiológico. Basta para ello formular un juicio de reproche dirigido a la víctima, por no haber sabido defender con vigor sus propios bienes jurídicos. Las consecuencias derivadas de esta visión –piénsese, por ejemplo, en los delitos contra la libertad sexual o contra el patrimonio– hacen inaceptable esta línea de razonamiento.
>
> Quien remite a una persona en la que confía una foto expresiva de su propia intimidad no está renunciando anticipadamente a ésta. Tampoco está sacrificando de forma irremediable su privacidad. Su gesto de confiada entrega y selectiva exposición a una persona cuya lealtad no cuestiona, no merece el castigo de la exposición al fisgoneo colectivo.–
>
> (…) Tiene razón el Fiscal al recordar que el requisito de la difusión quedó cumplido cuando, sin autorización de la afectada, se inició la cadena de difusión, siendo indiferente que la imagen sea remitida a una o más personas. Resulta contrario a las reglas de la lógica y a la intención del legislador, la exigencia de una difusión masiva en redes sociales de uso generalizado o la difusión simultánea a más de una persona por parte del receptor de las imágenes.–
>
> Cuestiona también la defensa que se haya producido un grave menoscabo de la intimidad de Joaquina. Se trata de un "... mero desnudo", alejado de cualquier connotación sexual o provocativa. Además, se dirigió por el acusado a un tercero –la entonces pareja de la víctima– que ya compartía intimidad con aquélla. No ha existido un verdadero perjuicio, pues la ruptura sentimental sobrevenida no estuvo relacionada con el envío de la fotografía».

---

[171] LLORIA GARCÍA, P.; «La difusión de imágenes íntimas sin consentimiento (A propósito de la Sentencia 70/2020 del Tribunal Supremo de 24 de febrero de 2020)», en *La Ley privacidad*, n.º 4, (abril-junio 2020), pp. 1-9.

Estas afirmaciones resultan de interés en la medida en que suponen aceptar, según la interpretación doctrinal[172] y jurisprudencial[173] mayoritaria, que resulta indiferente que la víctima enviara la imagen que autorizara a que el otro la tomara con su permiso, pues en ambos casos se cumplimenta el verbo típico y se consuma el delito. Por tanto, se sancionan dos conductas:

1. La de quien ha grabado el vídeo o hecho la fotografía con autorización y procede a difundir las imágenes sin consentimiento de la otra parte.
2. La de quien ha recibido las imágenes de otra persona y las reenvía o difunde sin consentimiento expreso del protagonista.

Sin embargo, esta doctrina en torno al significado del verbo típico «obtener» ha sido discutida por los votos particulares emitidos a dos sentencias que interpretaban en el mismo sentido que la comentada. Los votos emitidos a las STS núm. 699/2022, Sala 2ª, de lo Penal, de 11 de julio, Rec. 3204/2020 y STS núm. 767/2023, Sala 2ª, de lo Penal, de 3 de octubre, Rec. 5039/2021, discrepan de que se pueda incluir en el verbo obtener la conducta de enviar y recibir. En el caso de la primera resolución, todavía no se había incluido el tipo atenuado, por lo que el voto particular emitido, tras una serie de argumentos gramaticales y teleológicos, afirma que:

> «9. En resumen, el envío a un tercero de una foto íntima de una persona, que se obtiene por el remisor porque dicha persona se la ha entregado voluntariamente, sin precisarse el contexto de obtención, no cae dentro del tipo del artículo 197.7 CP».

El problema, que ya fue anunciado, radica en que, precisamente en ese momento, se encontraba en tramitación la reforma del tipo[174], que incluyó un tipo privilegiado que castiga a los que «*habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada»*, con una pena de multa de uno a tres meses.

Esta figura se introduce, aunque nada se dice en la exposición de motivos de la ley, con la intención de castigar a los redifusores, que no quedan incluidos en el tipo pues el sujeto activo, con la redacción original, sólo podía ser el sujeto que obtenía o recibía la imagen. La idea de castigar a quien difunde lo que ha recibido de otro, que no forma parte de la escena recogida en el material, había sido puesta de manifiesto por la doctrina[175], pero esta interpretación de los votos particulares la rechaza, no sólo para el tipo básico cuando era único, sino también para el caso del tipo atenuado, una vez que entró en vigor.

---

[172] LLORIA GARCÍA, P.; «La regulación penal en materia de violencia familiar y de género tras la reforma de 2015. Especial referencia al ámbito tecnológico», 2019, *Revista general de Derecho Penal*, n.º 31*.,* pp. 30-32.

[173] Vid., STS núm. 37/2021, Sala 2ª, de lo Penal, de 21 de enero, Rec.1074/2019, STS núm. 699/2022, Sala 2ª, de lo Penal, de 11 de julio, Rec.3204/2020 y STS núm. 767/2023, Sala 2ª, de lo Penal, de 3 de octubre, Rec. 5039/2021.

[174] BOE. Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual.

[175] DEVIS MATAMOROS, A.; «Aproximación jurisprudencial sobre la difusión de contenidos delictivos en redes sociales», *Diario La Ley,* 2022, n.º 10.153.

Sin embargo, la jurisprudencia ha adoptado la interpretación doctrinal. Así, en la STS núm. 767/2023, Sala 2ª, de lo Penal, de 3 de octubre, Rec. 5039/2021, que vuelve a contar con el voto particular de los mismos magistrados disidentes[176], se afirma:

> «Desde nuestro punto de vista, la Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual nada ha añadido al núcleo de la protección sustancial del precepto, sino que lo que efectúa es una incriminación de la conducta consistente en la redifusión o retuiteo de tales imágenes, por los terceros que las han recibido, naturalmente sancionando con menor pena a este comportamiento que la prevista para el autor de la difusión inicial, que es el que obtuvo inicialmente de la víctima la escena de contenido afectante de forma grave a la intimidad del mismo, y que sin su permiso o anuencia, la difunde a terceros, de cualquier modo que se produzca tal difusión, entre cuyos contornos fácticos admite cualquier exhibición, reenvío o redifusión a personas extrañas a la relación que permitió tal entrega exclusiva, por medio de la cual el agente obtuvo la imagen en cuestión».

---

[176] Donde afirman que, ante la ausencia de explicación en la norma, y atendiendo a criterios gramaticales y teleológicos en la exégesis, la aparición del tipo atenuado les permite reforzar su anterior interpretación, alegando que no es lo mismo obtener que recibir, y ello justifica la introducción del tipo atenuado. En este sentido aseveran:

> «La distinción entre el tipo básico (197.7.1º CP) y el novedoso tipo atenuado (197.7.2º) que debuta ahora en la agenda de este Tribunal, no radica en los verbos rectores (difundir, revelar, ceder sin consentimiento del afectado). Tampoco en el objeto material: imágenes o grabaciones audiovisuales obtenidas en algún lugar reservado con la anuencia del afectado idóneas para afectar gravemente a la intimidad.
>
> El elemento diferencial estriba en que en un caso es el sujeto activo quien ha obtenido las imágenes o grabaciones; y en el otro, de penalidad rebajada, no las ha obtenido; las ha recibido.
>
> No encontramos herramienta gramatical o léxica alguna para considerar que quien recibe del afectado, obtiene; y, sin embargo, quien recibe de otra persona, no obtiene, sino que sencillamente recibe. La única manera racional de coordinar ambos preceptos es considerar que obtener significa captar directamente; y recibir abarca todas las conductas en que el sujeto activo no ha intervenido en la captación o grabación de las imágenes o secuencia visual. El verbo recibir evoca una actitud pasiva del sujeto (tomar lo que le envían); obtener alberga un componente activo (conseguir lo que se pretende). Esa diferenciación, también en una perspectiva teleológica, encierra cierta lógica: se distinguen las conductas por su respectiva gravedad; aunque puede opinarse fundadamente que hay un punto mayor de antijuricidad en quien quebranta la confianza demostrada por el afectado al compartir con él su intimidad. Pero, en cualquier caso, no hay forma inteligible de sostener que quien recibe del afectado obtiene y quienes reciben de un tercero, no obtienen, sino que, en ese supuesto, solo reciben. O todos obtienen o todos reciben, pero no obtienen en el sentido del art. 197.7 CP. No encontramos otra fórmula para cohonestar ambos tipos. El primer acercamiento jurisprudencial a la norma (que se produjo a través de un pronunciamiento de Pleno),de forma comprensible y justificable pero un tanto voluntarista en nuestro modesto entender, quiso incluir en el tipo a quien recibía del afectado la imagen, defraudando esa confianza; pero, al mismo tiempo, reputó excesivo extender los tentáculos del precepto a terceros. Al paso de esa restricción jurisprudencial ha salido el legislador, haciendo ya gramaticalmente inviable ese dribling interpretativo que queda descalificado e imposibilitado por la reforma de 2022. Esta legislación, en ese sentido, resulta más favorable y aplicable retroactivamente. Por ello se confirió un trámite de audiencia a las partes al amparo de la Disposición Transitoria 9ª CP 1995.
>
> De entenderse sorteables los obstáculos de tipicidad resaltados en el apartado anterior de este voto, consideramos que los hechos debieran ser reubicados en el párrafo 2º del art. 197.7, norma posterior más beneficiosa que implícitamente ha extraído del párrafo anterior ese grupo de supuestos. El recurrente recibió; no obtuvo en el sentido del art. 197.7 CP. La pena debiera haberse reducido».

Siendo esto así, se puede afirmar que el artículo 197.7 castiga, por un lado, al que obtiene imágenes de contenido íntimo con autorización, y luego las difunde, cede o revela sin permiso dañando gravemente la intimidad de la persona afectada y, por otro, a quienes difunden las imágenes íntimas que han recibido de un tercero que obtuvo con autorización y difundió sin consentimiento. Esto es, se castiga a los redifusores.

El tipo agravado sanciona con mayor pena los casos en los que existe una relación de pareja o una situación de vulnerabilidad o ánimo de lucro. En este sentido, el precepto establece que se impondrá la pena en su mitad superior en los siguientes supuestos:

1. Cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia.
2. Cuando la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección.
3. O cuando los hechos se hubieran cometido con una finalidad lucrativa.

Hay que resaltar que el tipo agravado afecta a los dos tipos anteriores (el básico y el privilegiado), por lo que habrá que contemplar en todos los supuestos si concurren las circunstancias expuestas.

Por lo que hace a la primera agravación, supone tomar en consideración la idea de que se trata de un delito de violencia de género, según la tradicional interpretación de los mismos. En relación con la agravante relativa a las personas menores de edad, encuentra su fundamento en la mayor lesión que se deriva en el caso de ser personas menores de edad las víctimas de estos delitos, y se plantean problemas concursales, en relación con los delitos de *child grooming*. Del mismo modo, se discute hasta qué punto estas conductas tienen encaje en este delito, en la medida en que el consentimiento de los menores no es válido, por lo que resulta difícil de aplicar la figura que exige de consentimiento. La solución viene, o bien por adoptar una concepción amplia del consentimiento, o bien por reconducir estas acciones al artículo 197.1 en relación con el número 3 del mismo precepto.

Sería interesante trabajar esta cuestión, dado que, según datos recogidos por la ONG *Save The Children* en el informe «*Violencia viral. Resumen ejecutivo*» de 2019[177], este delito «*suele ocurrir a los 14 años por primera vez y la persona que con más frecuencia lo provoca es la chica o chico con quien salían*». Por su parte, el Instituto Nacional de Tecnologías de la Comunicación (INTECO), junto con Pantallas Amigas[178], en el estudio «Guía sobre adolescencia y sexting: qué es y cómo prevenirlo», refleja que prevalecen las víctimas chicas, mientras que son los chicos, los que mayoritariamente lo difunden.

---

177 SAVE THE CHILDREN. *Violencia viral resumen ejecutivo*, 2019. Disponible en: https://www.savethechildren.es/sites/default/files/imce/docs/violenciaviral_resumenejecutivo.pdf

178 INTECO. *Guía sobre adolescencia y sexting: qué es y cómo prevenirlo*, 2011. Disponible en: https://www.sexting.es/wp-content/uploads/guia-adolescentes-y-sexting-que-es-y-como-prevenirlo-INTECO-PANTALLASAMIGAS.pdf

5.3.2. Sextorsión

Tal y como se ha adelantado, la *sextorsión* se identifica con la acción de amenazar a otra persona (generalmente mujeres, niños, niñas o adolescentes) si no envía al agresor imágenes de naturaleza íntima, a riesgo de difundir otras de similar contenido que ya posea, con el consecuente agravio para la víctima. La diferencia con el *chantaje* radica, pues, en el tipo de amenaza si no se cumple la condición. No se trata de obtener dinero, como ocurre en otros casos que impropiamente se denominan *sextorsión*, como ya he dicho más arriba, sino más material erótico o sexual. Generalmente estas amenazas o coacciones se producen a través de sistemas de ciberacoso, por lo que, en ocasiones, se identifican con conductas de *child grooming* (fundamentalmente con el de embaucamiento del art. 183.2 CP y otras con conductas de pornografía infantil (captación del art. 189 CP).

A veces, también se identifica la *sextorsión* con la *porno-venganza,* conducta que afecta mayoritariamente a mujeres y que puede ser calificada también como amenaza condicional, aunque aquí la condición no consiste en recopilar más material gráfico, sino en que la mujer se someta a la voluntad del agresor (generalmente un hombre con el que tiene o ha tenido una relación afectiva). En estos casos, lo que se suele pedir a cambio de no difundir las imágenes que ya se poseen –bien con consentimiento, bien de forma ilegítima– es retomar la relación o aceptar determinadas condiciones en el pacto de separación o divorcio o cuestiones similares que, de no aceptarse, supondrán la difusión de imágenes de contenido erótico. Esta conducta, previa a la difusión ilegítima que quedaría castigada bien por el artículo 197 1, en relación con el artículo 197. 3 del CP, cuando no exista autorización para obtener o tener las imágenes, bien por el art. 197.7 CP, constituye un delito de amenazas condicionales básicas del art. 169 CP. Si no se cumple la condición (la mujer no se somete y no envía más imágenes), se está en presencia de un delito de amenazas condicionales básicas, mientras que si se consigue el propósito (esto es, la mujer envía más imágenes, para evitar la difusión de las previas), el delito será de amenazas condicionales agravadas.

El problema surge cuando la difusión de los *deepFakes pornográficas.* En este caso, mientras no se tipifique como delito, o entendemos que estas acciones se pueden castigar como un atentado a la integridad moral, o no podrán formar parte de los delitos de amenazas de mal que constituya delito.

La sextorsión y la pornovenganza, se presentan entonces como situaciones previas a la comisión del delito de difusión de imágenes íntimas (obtenidas con o sin consentimiento –arts. 197.7 y 197.1 y 3, respectivamente) y cumplimentarán tipos delictivos únicos de amenazas. Si, por el contrario, la sextorsión o la porno-venganza van más allá de la situación amenazante y se llega a producir la difusión de imágenes de manera posterior, concurrirán los delitos de estafa en concurso real (generalmente, con dudas en los casos de *child grooming*), con los correspondientes atentados contra la intimidad o contra la indemnidad sexual de las personas menores de edad, en su caso.

Todo ello, además, conduce a afirmar que con la normativa actual quedan cubiertas, de momento, las acciones de sexting ajeno, sextorsión y pornovenganza, cuando el agresor utiliza imágenes reales, bien para amenazar, bien para difundir, pues basta reinterpretar las figuras con las que ya cuenta

nuestro CP, tomando en consideración el nuevo entorno digital y las implicaciones que ello trae para el principio de lesividad y el de proporcionalidad en el ámbito punitivo[179].

En relación con estas acciones, se puede diferenciar por el modo de llevarlas a cabo, las siguientes conductas:

- *Sextorsión:* se utilizan imágenes íntimas, tanto vídeos como fotos, para chantajear a una persona. Se le amenaza con difundirlas si no se obtiene alguna contrapartida como, por ejemplo, dinero, favores sexuales, ventajas profesionales, etcétera. Se considera que no existe un consentimiento válido, ni voluntariedad en la conducta. El término *sextorsión* incorporado en la ya citada STEDH, caso BUTURUGA c. Rumanía, de 11 de junio de 2020, fue citado por primera vez por la Sala 2ª de lo Penal del Tribunal Supremo en la Sentencia núm. 450/2018, de 10 de octubre, Rec.2547/2017.
- *Slutshamming o tildar de prostituta:* es la práctica de criticar y/o culpabilizar a mujeres y niñas por portarse de una manera que algunos perciben como promiscua o fuera de los roles tradicionales de género. En los medios electrónicos, ese tipo de violencia puede ocurrir a través de las redes sociales e incluso ir asociada a la «venganza pornográfica».
- *Sex-casting*: consiste en la grabación de imágenes sexuales mediante webcam y su posterior difusión por redes sociales, mail o servicios de mensajería instantánea.

Si se llegan a difundir las imágenes, estaríamos ante un supuesto de afectación a la intimidad, bien por el tipo genérico si no hay consentimiento (art. 197.1 y 3), bien por el tipo específico si lo hay (art. 197.7), que también se podría reconducir, si fuera necesario, a los atentados contra la integridad moral del art. 173. Todo ello, en concurso con el correspondiente delito de amenazas al que se ha hecho referencia anteriormente.

Merece la pena resaltar que, además de la vulneración de la intimidad en relación con la imagen, en los casos de violencia cometida dentro del seno de la pareja o expareja son cada vez más frecuentes los supuestos en los que el sujeto activo quiebra las barreras de protección de un dispositivo electrónico para conocer las conversaciones y mensajes de sus parejas, tanto su contenido como sus destinatarios, o para acceder a sus archivos. Es lo que se conoce como violencia de control.

Así, es conocido –y su uso ha dado lugar a la incoación de diversos procedimientos judiciales– el denominado programa «*Cerberus*» que, instalado directamente por el agresor en el teléfono móvil de su víctima, hace factible el control y vigilancia de la actividad del terminal y, en consecuencia, de la persona afectada a través del conocimiento de las llamadas entrantes y salientes, la geolocalización del dispositivo e, incluso, la obtención de fotografías o de grabaciones en vídeo y audio realizadas desde la cámara del móvil controlado[180]. Estos supuestos son casos de acoso, que se recogen en el

---

[179] LLORIA GARCÍA, P.; «Sexting y sextorsión: dos modalidades delictivas con sesgo de género», en ibericonnect.blog, 2023. Disponible en: https://www.ibericonnect.blog/2023/07/sexting-y-sextorsion-dos-modalidades-delictivas-con-sesgo-de-genero/

[180] BOE. Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos, 2017. Disponible en: https://www.boe.es/buscar/abrir_fiscalia.php?id=FIS-C-2017-00003.pdf

art. 172 ter del CP, y también se establece la posibilidad de castigar si se entiende que previamente se ha cometido un delito de intrusismo informático a quien, sin estar debidamente autorizado, produzca, adquiera para su uso o facilite a terceros un programa informático concebido para cometer estos delitos, incluyendo una contraseña de ordenador, código de acceso o elementos similares que permitan acceder a un sistema informático (artículo 197 ter CP).

De esta manera, se penaliza incluso la mera adquisición de esos programas o contraseñas, siempre que exista un dolo específico en relación con la situación de vulneración de la intimidad. Si, además, se instala en el móvil de otro y se descubre su intimidad, se podría condenar a penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses, por el delito de descubrimiento y revelación de secretos.

Esta forma de violencia puede ocurrir en una gran variedad de contextos y relaciones interpersonales: en una relación íntima y de confianza, en la cual estas imágenes o informaciones son enviadas de forma voluntaria por una persona a su pareja o expareja sentimental, por amistades, conocidos o desconocidos, o cuando el material se obtiene mediante *hackeo* o acceso físico a dispositivos. En este caso, ya no es difusión de *sexting* ajeno, sino que entrarían en juego delitos tales como el de revelación de secretos del artículo 197.1, el intrusismo informático del artículo 199, o alguna de las figuras de acoso contempladas en el art. 172 ter, todos ellos del CP.

Entre la jurisprudencia, destaca una de las primeras sentencias que introdujo la denominación de sextorsión, la STS núm. 377/2018, Sala 2ª, de lo Penal, de 23 de julio, Rec. 10036/2018, que condena por delitos continuados de abuso sexual, contra la intimidad y de amenazas. En este asunto, el agresor accedió a los ordenadores de las víctimas utilizando un virus para obtener archivos personales de las mujeres, con el fin de utilizarlos para amenazarlas con divulgar fotos o vídeos comprometedores si las víctimas se negaban a mantener relaciones virtuales de carácter sexual con él. El fallo analiza en profundidad el delito de abusos sexuales cometido por Internet. Ello supone, evidentemente, que la víctima se ve obligada a realizar autocontactos sexuales, lo que, en el caso de las personas adultas, no se puede castigar. Sin embargo, en relación con los menores, el Alto Tribunal entiende que es innecesario el contacto sexual directo, siendo suficiente las acciones orientadas a atentar contra la libertad sexual de las víctimas. Según sea la conducta sexual requerida por el autor en estos casos, podría encajarse dentro de los artículos 178.2 o 179 del Código Penal.

5.4. *Delito de incitación al odio*

Se regula en el artículo 510 del Código Penal. Aunque es un término amplio vinculado a la violencia contra grupos por sus condiciones étnicas, religiosas o de origen, también se registra contra las mujeres e implica sexualización, cosificación y comentarios degradantes sobre el aspecto físico o intelectual, así como amenazas de violación.

Pueden consistir en actos intencionales para censurar y dañar a organizaciones de mujeres, incluso con ataques a sus canales de expresión, como tener acceso a ellos sin consentimiento y *hackear* páginas de Internet, redes sociales o cuentas de correo para afectar el desarrollo de sus funciones, lograr que la mujer abandone las redes sociales personales o de la organización, bien mediante el uso de

normas comunitarias para denunciar contenido que la plataforma considera sensible, o bien mediante ataques de denegación de servicio, restricciones de uso de dominio o robo de dominio, y apagones de conexión a Internet durante una reunión o protesta.

Este artículo establece penas de prisión de 1 a 4 años y multa de 6 a 12 meses para aquellos que promueven, incitan o fomentan el odio, la discriminación o la violencia contra grupos o personas por motivos racistas, antisemitas, o por motivos de orientación sexual, ideológica, religiosa o sexual, así como a quienes produzcan o distribuyan material que pueda incitar al odio. Igualmente, se castiga con la pena de prisión de 6 meses a 1 año y multa de 6 a 12 meses al que enaltezca delitos cometidos o lesione la dignidad de una persona mediante acciones que entrañen los motivos indicados. Las penas se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de Internet o mediante el uso de tecnologías, de modo que aquel se hiciera accesible a un elevado número de personas.

Un ejemplo del delito de odio es el reseñado en la STS núm. 72/2018, Sala 2ª, de lo Penal, de 9 de febrero, Rec. 583/2017. En el fallo se condena a un internauta que publicó a través de una red social distintos mensajes que incitaban al odio. La sentencia reflexiona sobre la importancia de la libertad de expresión, pero también reconoce la necesidad de sancionar expresiones que fomenten el odio y la violencia. El Tribunal destaca que el dolo en estos delitos no requiere un elemento específico, sino que basta la constatación de un dolo básico, es decir, voluntariedad y ausencia de una reacción incontrolada o momentánea ante un estímulo externo. En el caso analizado, el Tribunal alude a que las manifestaciones vertidas por el agresor se producen en distintas fechas, lo que indica una voluntariedad en su conducta y no una reacción puntual o incontrolada. Además, el contenido de las frases entraña agresividad y odio, especialmente hacia las mujeres, por lo que el autor conocía y quería realizar las expresiones que publicó en la red social.

El uso masivo de redes sociales y aplicaciones de mensajería ha propiciado el incremento de conductas como el del delito de incitación al odio, que se trata de una conducta que atenta contra derechos fundamentales y libertades básicas.

6. CONCURRENCIA ENTRE DELITOS

Los delitos tecnológicos más habituales y de los que se ha dado cuenta en el epígrafe anterior pueden concurrir con otros que, sin ser tampoco específicamente tecnológicos, en el entorno virtual suelen ser habituales. Fundamentalmente se trata de los delitos de amenazas y coacciones, generalmente vinculados a las situaciones de control que sufren las mujeres y las personas menores de edad en el ciberespacio.

En España, las amenazas y coacciones constituyen el segundo grupo de ciberdelitos más denunciados, sólo superados por el ciberfraude[181]. Suele ser común, por ejemplo, amenazar con causar daños físicos o propagar información particular que pueda dañar la intimidad de la víctima. Las penas se ven

[181] CANO TERUEL, Q.; «Ciberdelencuencia en el Código Penal», *cibercrim*, 2024. Disponible en: https://cibercrim.com/ciberdelincuencia-en-el-codigo-penal/

agravadas si las amenazas se hicieran por escrito, por teléfono o por cualquier medio de comunicación o reproducción, según lo que establece el artículo 169 CP, por lo que las amenazas realizadas a través de medios de comunicación social o plataformas interactivas entrarían dentro de esta idea de amenazas hechas con publicidad.

En el caso de las amenazas (art. 169 a 171 CP), las conductas en el entorno virtual no distan de las del físico, aunque pueden ser más lesivas, por razón de la indefensión que genera, si bien cabe destacar como habitual el chantaje que se produce cuando, por ejemplo, el autor obtiene una imagen comprometida de la víctima y amenaza con difundirla si esta no le recompensa con alguna cantidad económica o similar (art. 171.2 CP).

Las situaciones de lo que se ha venido a denominar «sextorsión» generalmente encuentran cobertura entre los delitos de amenazas en su modalidad de amenaza condicional, ya que la tenencia de imágenes íntimas se utiliza para promover el chantaje a la víctima, con el fin de ejercer control y dominio bajo la advertencia de que, si no se somete a lo pedido, se difundirán aquellas imágenes que la víctima no desea que salgan a la luz pública. La condición suele ser la de tener relaciones sexuales, pero también pueden exigirse otras acciones, como, por ejemplo, retomar la vida de pareja, o permitir estar con los hijos e hijas cuando alguna medida judicial lo impide o condiciona.

Las amenazas a través de aplicaciones se llevan a cabo de forma frecuente, ejemplo de ello es el asunto tratado por la STS núm. 300/2015, Sala 2ª, de lo Penal, de 19 de mayo, Rec. 2387/2014[182]:

> *«En fecha 3 de junio de 2013, el procesado, que se encontraba en busca y captura ordenada por el Juzgado de Violencia contra la mujer n° 5 de Barcelona, envió al teléfono móvil de Cristina varios mensajes de texto a través del sistema "wechap" (versión china del whatsapp), con intención de amedrentarla, generándole el tenor de sufrir un atentado contra su vida o la de su familia, con el siguiente contenido:*
>
> – a las 19,41 h: "te iré a buscar otra vez, no lo dudes...je je, entonces tu hermano también está protegido por vehículo policial?, ¿la tienda de tu tía también ha cerrado?... cuando tu familia sale de casa también está protegida por vehículo policial?"
>
> – a las 19,47 h: "no tengas miedo, navega por internet, come, duerme, habrá algún momento en el que tendrás miedo...24 horas con la policía! ¡a ver cómo aguanta tu familia! tu casa en China también está protegida por la policía? empezaré con tu hermano mayor, dile que tenga cuidado, ya queda poco para las vacaciones, sería una lástima que perdiera un brazo o una pierna...ya veré de qué es capaz tu policía.
>
> – a las 19.57 h: "no temas a las pesadillas, no me pidas que perdona a tu familia cuando ocurra algo, pídele a la Policía que proteja a tu familia cuando ocurra algo".

---

[182] La Audiencia de instancia dictó el siguiente pronunciamiento:
«(…) CONDENAMOS a Adriano como autor de un DELITO DE AMENAZAS GRAVES, concurriendo la agravante de parentesco, a la pena de un año y seis meses de prisión, y la prohibición de aproximación a Cristina en distancia inferior a 1000 metros, así como a su domicilio o lugar de trabajo, así como de comunicar con la misma por cualquier medio por tiempo de un año superior a la pena privativa de libertad impuesta por este delito. Imponemos al procesado el abono de las costas procesales, incluidas las de la acusación particular».

El Juzgado de Violencia sobre la mujer n° 9 de Madrid acordó la prisión provisional comunicada y sin fianza de Adriano por Auto de fecha 16 de junio de 2013, ratificada por Auto de fecha 20 de junio de 2013 del Juzgado de Violencia sobre la Mujer n° 5 de Barcelona. Adriano ha sido suspendido en el ejercicio de la patria potestad sobre su hija que tiene en común con la Sra. Cristina en virtud de Auto de fecha 30 de abril de 2013 del Juzgado de Violencia sobre la Mujer n° 5 de Barcelona».

Por lo que hace a las coacciones, la conducta, como es sabido, consiste en obligar a alguien a hacer algo que no quiere o impedirle hacer lo que quiere, que se regula en los artículos 172 a 172 ter del CP. El primero alude a las coacciones genéricas, mientras que los siguientes contemplan casos de coacciones específicas. En estas conductas, sucede como con las amenazas. Se trata de delitos de medios indeterminados que pueden llevarse a cabo, también, mediante el instrumento tecnológico, sin necesidad de una distinción normativa entre estas y las que se producen en el mundo físico.

En relación con las acciones de violencia de género, el delito de coacciones concurrirá, por ejemplo, cuando se extorsiona a la víctima con que, en caso de no acceder a las pretensiones del agresor (como puede ser la continuidad de la relación de pareja o el mantenimiento de relaciones sexuales), este procederá a la difusión, bien en la *web*, bien en el ámbito de sus familiares y/o amigos, de imágenes de contenido íntimo en la que aquella aparece. Si no se difunden finalmente las imágenes, pero se consigue el propósito, esta conducta será constitutiva de un delito de coacciones del artículo 172 (si no constituye una amenaza condicional), dada la gravedad de la coacción y del enorme peligro de difusión indiscriminada derivada de la inserción en la *web* de momentos íntimos. Y si se procediera a la efectiva difusión de las imágenes, este hecho sería constitutivo de un delito de *sexting* de tercero del artículo 197.7 CP en concurso con el delito de coacciones.

Cuando la información o las imágenes se obtienen sin consentimiento de la persona afectada, el delito ya no es el del art. 197.7 sino un delito de revelación de secretos e informaciones de los contemplados en el art. 197 en sus primeros números. La STS núm. 15/2023, Sala 2ª, de lo Penal, de 19 de enero, Rec.4891/2020, hace referencia a la falta de consentimiento en la obtención del material y condena por un delito de descubrimiento y revelación de secretos del artículo 197.1 y 4 b) del Código Penal, concurriendo como agravante la circunstancia mixta de parentesco del artículo 23.

Pueden darse estas conductas en concurso con otras tipologías delictivas, como es el caso juzgado en la STS núm. 871/2022, Sala 2ª, de lo Penal, de 7 de noviembre, Rec. 10258/2022[183].

---

[183] En la citada sentencia se dictó el siguiente pronunciamiento:
«DEBEMOS CONDENAR y CONDENAMOS al acusado Demetrio, de las circunstancias ya expuestas, como responsable en concepto de autor de los siguientes delitos: A) Un delito continuado de elaboración de pornografía infantil del art. 74, 189.1.a) y 189.2.a) y g) del Código Penal; B) Un delito de descubrimiento y revelación de secretos del art. 197.1 y 5 del Código Penal y C) Un delito de distribución de pornografía infantil del art. 189 1.b) del Código Penal (EDL 1995/16398); Concurriendo en los dos primeros delitos la circunstancia modificativa de la responsabilidad criminal del art. 23, mixta de parentesco, IMPONEMOS al acusado Demetrio, las siguientes penas: A) Por el delito continuado de elaboración de pornografía infantil: OCHO AÑOS DE PRISIÓN, inhabilitación especial para el ejercicio de sufragio pasivo durante el tiempo de la condena, INHABILITACIÓN ESPECIAL PARA EMPLEO O CARGO PÚBLICO O EJERCICIO DE CUALQUIER OFICIO O PROFESIÓN

Otros tipos delictivos que podrían resultar de aplicación, en concurso con el correspondiente delito cometido a través de las nuevas tecnologías con sus correspondientes penas, serían el delito de trato degradante del artículo 173 CP para dañar la dignidad de otra persona, obligar a realizar actos humillantes, el de agresiones sexuales de los artículos 178 a 183 CP[184] y el de corrupción de menores (artículo 188-189 CP).

Asimismo, el *ciberbullying* o ciberacoso psicológico, cuando se produce dentro de una relación de pareja, puede ser constitutivo de un delito de maltrato habitual del artículo 173.2 del Código Penal, sin perjuicio de los concursos concretos con los delitos por los actos de violencia que sean por sí mismos constitutivos de infracción penal.

Estas conductas de ciberacoso pueden suponer delitos contra el honor que puede verse lesionado, encuadrándose en los delitos de calumnias e injurias. La calumnia, prevista en el art. 205 CP, consiste en la imputación de un delito con conocimiento de su falsedad. La injuria, tipificada en el art. 208 CP, es la acción expresión destinada a mermar la dignidad personal (por ejemplo, mediante insultos). Un elemento destacable que agrava las penas de ambos tipos es el de la publicidad, que suele concurrir cuando se difunden los mensajes a través de, por ejemplo, redes sociales o grupos de mensajería (art. 211 CP).

7. LA TRATA DE PERSONAS Y EL USO DE LAS TECNOLOGÍAS

La trata de seres humanos se presenta como uno de los crímenes más graves que se producen en nuestra sociedad y ello, fundamentalmente, porque la compra y venta de seres humanos afecta a

---

QUE PUEDA TENER RELACIÓN CON MENORES DE EDAD por tiempo de ONCE AÑOS de conformidad con el art. 192 núm. 3 del Código Penal (EDL 1995/16398); LIBERTAD VIGILADA durante SEIS AÑOS conforme a lo dispuesto en el art. 192 núm. 1 del Código Penal (EDL 1995/16398) y éste en relación con lo dispuesto en el art. 106 núm. 1- j del mismo texto legal y la PROHIBICIÓN DE APROXIMACIÓN A LA MENOR Esmeralda., tanto a ella, como a su domicilio y lugares que habitualmente frecuente a una distancia de 500 metros, así como la PROHIBICIÓN DE COMUNICARSE CON ELLA por cualquier medio o procedimiento por un tiempo de diez años, de conformidad con los arts. 57.1 en relación con el art. 48 CP. B) Por el delito de descubrimiento y revelación de secretos TRES AÑOS DE PRISIÓN, inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de condena y MULTA DE VEINTE MESES a razón de una cuota diaria de 6 euros, y C) Por el delito de distribución de pornografía infantil UN AÑO DE PRISIÓN, inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de condena, INHABILITACIÓN ESPECIAL PARA EMPLEO, CARGO PÚBLICO O EJERCICIO DE CUALQUIER OFICIO O PROFESIÓN QUE PUEDA TENER RELACIÓN CON MENORES DE EDAD por tiempo de CUATRO AÑOS y UN AÑO de LIBERTAD VIGILADA de conformidad con el art. 192 núm. 1 del Código Penal (EDL 1995/16398) y éste en relación con lo dispuesto en el art. 106 núm. 1- j del mismo texto legal, posterior a la prisión. Se acuerda el comiso de los efectos intervenidos al acusado a los que se dará el destino legal. Se imponen al acusado las costas procesales».

[184] Vid.; STS núm. 447/2021, Sala 2ª, de lo Penal, de 26 de mayo, Rec. 3097/2019, que como habíamos mencionado en párrafos anteriores, recoge la condena por un delito de agresión sexual agravada, basándose en pruebas que muestran que el agresor utiliza su teléfono móvil para contactar con una menor, solicitándole imágenes pornográficas y amenazándola. El Tribunal determina que la conducta del acusado constituye agresión sexual agravada por la minoría de edad de la víctima. La sentencia destaca el tratamiento de la ciberintimidación como forma de intimidación equiparable a la violencia física en delitos de agresión sexual, adaptando la interpretación del derecho penal a los contextos digitales y la protección de menores en el ámbito *online*.

múltiples bienes jurídicos fundamentales: la vida, la salud, la integridad física o psíquica, la libertad, la libertad sexual, la integridad moral, siendo que siempre se ve afectada la dignidad, como elemento *quasi* definidor del hecho de la trata[185]. Estos bienes jurídicos se ven lesionados o puestos en peligro (conjunta o independientemente) sin importar la finalidad de explotación que acompaña a la trata; afección a la que se suma la que se derive del concreto acto de explotación (sexual, laboral, delictual, etc.) que finalmente se produzca si la persona no es liberada durante el proceso que culminará con su esclavitud.

Además, estas conductas implican una situación global que afecta a un numerosísimo grupo de personas en todo el mundo, aunque los datos exactos sean difíciles de concretar debido a la importante cifra negra[186] que rodea a estos delitos, fundamentalmente por el desconocimiento que tienen las víctimas de los medios de denuncia y defensa de que disponen en el país en el que se encuentren, así como por el miedo que padecen tanto como consecuencia de las amenazas y malos tratos que sufren a manos de los agresores, como por el temor que se deriva de su situación de ilegalidad en el país de recepción y tránsito.

Ciertamente, aunque los fines de explotación son variados, la trata no es un fenómeno objetivamente neutro, desde el punto de vista del género. Así se afirma, entre otros documentos, en el *Plan integral de lucha contra la trata de seres humanos con fines de explotación sexual*[187], aunque las mujeres y las niñas también son víctimas de otro tipo de explotación que quizá aún no ha sido analizada, en la que habría que incluir, por ejemplo, la trata para llevar a cabo actos de gestación por sustitución. En todo caso, las prácticas de explotación sexual (prostitución y pornografía coactiva, fundamentalmente) vienen vinculándose de manera particularmente relevante al hecho de la trata de mujeres y niñas. En este sentido, recientemente la Relatora Especial de la ONU, en su Informe sobre *Prostitución y violencia contra las mujeres y las niñas*, ante la disparidad de criterios para identificar la prostitución, opta por identificarla con un sistema de violencia para someter a mujeres y niñas, cosificándolas, sobre la base de la desigualdad[188] que, sin duda, tiene una dimensión mundial.

Si a la relación con la globalización y la transnacionalidad unimos el incremento en el uso de las TIC, se pone en evidencia una de las causas del preocupante crecimiento del fenómeno, al que también

---

185 Tal y como se señala en la sentencia TEDH, Asunto Rantsev c. Chipre y Rusia (Demanda 25965/04, de 7 de enero de 2010), se vincula la trata de seres humanos con la vulneración de la dignidad humana, cuando se afirma que no cabe duda «*de que la trata de personas amenaza la dignidad humana y las libertades fundamentales de sus víctimas y no puede ser considerada compatible con una sociedad democrática y los valores expuestos en el Convenio».*

186 UNODC. Se estima en 2,5 millones el número de personas víctimas de la trata. Sin embargo, se calcula que, por cada víctima de la trata de personas identificada, existen 20 más sin identificar. Disponible en https://www.unodc.org/documents/lpo-brazil/sobre-unodc/Fact_Sheet_Dados_Trafico_de_Pessoas_geral_ESP.pdf

187 ESPAÑA. Ministerio de Igualdad. Instituto de Mujeres, 2022. Disponible en: https://www.inmujeres.gob.es/areasTematicas/multiDiscriminacion/mujeresVuln/docs/plan.pdf

188 ONU. *La prostitución y la violencia contra las mujeres y las niñas. Informe de la Relatora especial sobre la violencia contra las mujeres y las niñas, sus causas y consecuencias*, 2024, p. 2. Disponible en: https://documents.un.org/doc/undoc/gen/g24/078/84/pdf/g2407884.pdf

alude la relatora en su informe[189], que no es otra que la dificultad en la persecución de estos delitos, sin olvidar que los mismos se configuran en el ordenamiento interno, desde el punto de vista de su naturaleza jurídica, como iterativos que se prolongan en el tiempo y en el espacio, y esto lleva a que en ocasiones sea del todo punto imposible el rastreo de los tratantes por los propios cuerpos policiales. Teniendo en cuenta, además, que las acciones de trata están íntimamente relacionadas con la criminalidad organizada, los Estados se ven obligados a adoptar soluciones normativas comunes, con la finalidad de dotar de unidad al castigo y facilitar la lucha contra los autores del crimen.

En este sentido, hay que recordar que, hasta hace poco, las legislaciones adoptaban un punto de vista criminocéntrico, que fijaba el foco en la punición del proceso de traslado, lo que se traducía en la revictimización de las personas tratadas, ya que algunas de sus circunstancias, como la diferencia de idioma, cultura o religión, conducía, en no pocas ocasiones, a no identificar correctamente a las víctimas de trata y confundirlas con inmigrantes ilegales que se desplazan voluntariamente. Como es común advertir, esta orientación lleva a que el objetivo principal sea el delito y que su castigo se presente como la máxima aspiración. Este entendimiento, que se corresponde con las primeras consideraciones de la trata desde el punto de vista normativo, cambia con la aprobación del Protocolo de Palermo. Desde este momento, y como solución alternativa a estas cifras tan elevadas de personas sometidas a la trata, la doctrina solicita que la cuestión se aborde desde un prisma que atienda a las necesidades de la víctima (sin descuidar la vertiente punitiva) a través de la denominada «política de las 3P» (prevención, persecución, protección) y que tome como referencia la perspectiva de los derechos fundamentales de las víctimas[190].

Este es, además, el mandato que contiene la Directiva 2011/36/UE, de 5 abril de 2018, que recoge lo que ha se venido a llamar una orientación victimocéntrica, cuando establece la visión integrada y global como requisito para alcanzar una lucha más eficaz frente a esta realidad criminal. Esta norma ha sido recientemente modificada por la Directiva (UE) 2024/1712 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por la que se modifica la Directiva 2011/36/UE relativa a la prevención y lucha contra la trata de seres humanos y a la protección de las víctimas[191]. Con la misma no se pierde esta visión centrada en la víctima, sino que, por el contrario, se intenta reforzar atendiendo al origen multicausal de la trata y tomando en consideración una visión interseccional de la discriminación, y poniendo de manifiesto la necesidad de mejora de las diferentes normativas en ámbitos tan diversos como la detección temprana, la responsabilidad de las personas jurídicas o el hecho del uso de las tecnologías para la comisión de los delitos de trata de seres humanos.

En relación con este último punto, que es el que afecta a este epígrafe, la propia Directiva recuerda que ya se reconocía la influencia de las TIC en el texto original de 2011 (para la captación, la explotación

---

189 *Ibidem,* p. 18.

190 SERRA CRISTÓBAL, R.; «La trata de mujeres como una de las formas más atroces de violencia contra la mujer», en MARTÍN SANCHEZ, M.; (Dir.): «Estudio integral de la violencia de género; un análisis teórico-práctico desde el Derecho y las Ciencias Sociales», Valencia, Tirant Lo Blanch, 2018, pp. 271-292.

191 UE. Directiva (UE) 2024/1712 del Parlamento Europeo y del Consejo, de 13 de junio de 2024. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80945

o el control de las víctimas). Sin embargo, resulta recomendable actualizar esta visión y abarcar también, por un lado, la mayor lesión para los bienes jurídicos que se deriva del uso de redes sociales en el momento de la explotación (por las propias características de los delitos tecnológicos[192]) y, por otro, mejorar la formación de los cuerpos policiales para interferir en los procesos de captación, explotación y control de las víctimas, así como la publicación y difusión de los materiales obtenidos de la explotación, sin olvidar que la tecnología dificulta enormemente la persecución, entre otras razones, porque hace más difícil relacionar a los diferentes sujetos que intervienen en el delito y su relación con la víctima.

La Directiva dispone que el sistema penal en lo relativo a la trata de seres humanos debe establecer penas que reflejen la gravedad de las conductas delictivas y el impacto negativo que estas tienen en las víctimas. Esto implica que las penas deben ser más severas para aquellos delitos que causan un daño más profundo y duradero. Un aspecto importante de este daño es la difusión de material que esté relacionado con la explotación de las víctimas, ya que esta propagación puede agravar el sufrimiento de las mismas. Por lo tanto, es fundamental que se considere la difusión de *«imágenes, vídeos o material similar de carácter sexual que impliquen a la víctima»* como una circunstancia agravante en la legislación. Esto significa que, si alguien difunde dicho material a través de tecnologías de la información y comunicación, esto debería ser tratado con mayor severidad en términos de penas. Sin embargo, los Estados miembros tiene la flexibilidad de no estar obligados a incluir esta circunstancia agravante si, en su legislación nacional, ya existe una penalización específica para la difusión de este tipo de material. En tal caso, si la infracción se considera un delito independiente y puede resultar en penas más severas según el derecho nacional[193], no sería necesario añadir una agravante, lo que permite a cada país adaptar su legislación a sus propias circunstancias y necesidades.

Por lo tanto, y a pesar de las advertencias del Grupo de Expertos sobre la lucha contra la trata de seres humanos (GRETA)[194], en relación con la necesidad de no centrar los esfuerzos de la lucha contra la trata exclusivamente en el ámbito de la explotación sexual, la Directiva del año 24 toma la misma línea que el Informe de la Relatora especial, en el que, entre las recomendaciones que hace a los Estados con respecto a la pornografía y otras formas de prostitución[195], facilitadas por las plataformas digitales, se encuentran las siguientes:

---

192 LLORIA GARCÍA, P.; «Algunas reflexiones sobre el concepto de delito tecnológico y sus características» en LEÓN ALAPONT, J., GONZÁLEZ CUSSAC, J.L.; «Estudios jurídicos en memoria de la Profesora Doctora Elena Górriz Royo», Valencia, Tirant lo Blanch, 2020.

193 UE. Directiva (UE) 2024/1712 del Parlamento Europeo y del Consejo, de 13 de junio de 2024. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2024-80945

194 CONSEJO DE EUROPA. *Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Spain*, GRETA, 2018. Disponible en https://rm.coe.int/greta-2018-7-frg-esp-en/16808b51e0 GRETA es el responsable de la supervisión sobre la implementación por los Estados Parte del Convenio del Consejo de Europa sobre la eliminación de la trata de seres humanos.

195 *Ibidem*. El informe vincula ambas realidades y cualquier otro tipo de explotación sexual, siempre en el ámbito de la trata, por lo que se entiende que deben ser coactivas.

«a) Adoptar normativas que ataquen de manera integral los contenidos pornográficos y penalicen explícitamente la posesión, la producción o el alojamiento de material, ya que atentan contra el derecho a la vida y a la dignidad y constituyen tortura o trato inhumano o degradante; adoptar legislación internacional para abolir la pornografía y su consumo; retirar inmediatamente las imágenes sexuales de menores y la pornografía facilitada digitalmente que pueda ser accesible de cualquier forma a menores; e imponer su cumplimiento en todo el sector;

b) A la espera de la abolición de la pornografía, aplicar un estricto sistema de verificación de la edad en toda la pornografía en línea, sistemas rigurosos de moderación, etiquetado y advertencia, y un filtrado obligatorio por parte de los proveedores de servicios de Internet con opciones de inclusión voluntaria para adultos; y sancionar a los sitios de pornografía y redes sociales que alberguen contenidos pornográficos ilegales»[196].

De la misma manera, la Relatora Especial se pronuncia sobre la cibertrata transfronteriza, apuntando que

«*se recoja el intercambio transfronterizo de pruebas en cualquier pacto digital de las Naciones Unidas o tratado internacional futuros, y abordar explícitamente la explotación sexual en línea; a falta de un tratado internacional sobre ciberdelincuencia, adoptar el Convenio sobre la Ciberdelincuencia para abordar las responsabilidades en el ámbito de los ciberdelitos, incluida la prevención de la explotación sexual infantil facilitada por la tecnología*»[197].

Centrándonos en el ordenamiento jurídico español, la trata con fines de explotación sexual está regulada en el artículo 177 bis, del Código Penal. Queda consumado el tipo delictivo una vez se haya producido la captación dirigida a cualquier propósito de los tipificados en el 177 bis CP, aun cuando no se lleve a cabo dicha explotación; el elemento nuclear reside en la falta de consentimiento invalidado por violencia o intimidación o situación de necesidad o por otras causas que llevan a entender la ausencia de este. En esta línea, una situación de necesidad económica, tal y como además señala el artículo, impide a las víctimas poder emitir un consentimiento libre y voluntario. Por ello, el delito de trata está conectado con la lesión a la dignidad de la persona y constituye un atentado a los derechos más esenciales[198]. El consentimiento o aprobación de la persona objeto de trata evidentemente resulta inválido si se detecta una situación de vulnerabilidad en las víctimas.

Si bien es cierto que no se recogen todavía agravaciones específicas en relación con el uso de la tecnología para la difusión de materiales que contengan situaciones de explotación sexual a través de redes sociales o mediante el instrumento tecnológico, no es menos cierto que sí se puede castigar la tenencia en el caso de menores. Habrá de estudiarse hasta qué punto esta conducta entra o no

---

[196] ONU. *La prostitución y la violencia contra las mujeres y las niñas. Informe de la Relatora especial sobre la violencia contra las mujeres y las niñas, sus causas y consecuencias*, 2024, p. 2. Disponible en: https://documents.un.org/doc/undoc/gen/g24/078/84/pdf/g2407884.pdf

[197] *Ibidem*, pp. 18-19.

[198] VILLACAMPA ESTIARTE, C.; «La trata de seres humanos tras la reforma del Código Penal de 2015», *Diario La Ley*, 2015, n. 8554, pp.13.

en el ámbito de protección de los delitos de difusión de imágenes íntimas (obtenidas con o sin consentimiento) y valorar la necesidad de modificación de la normativa penal en esta materia.

Por otro lado, no se afirma en vano que la trata de mujeres con fines de explotación sexual o laboral es una manifestación de la violencia de género, entendiendo como tal, todos aquellos actos que afectan a las mujeres de forma desproporcionada.

Atendiendo a la situación de vulnerabilidad de la víctima previa a la captación, debemos de tener en cuenta que los métodos utilizados por las organizaciones criminales van perfeccionándose progresivamente, donde cada vez se utilizan más instrumentos *online* a través de páginas *web* y redes sociales, sin olvidar cómo la tecnología facilita 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.

Como ya se ha expuesto, el proceso que se deriva de todo acto de trata ha evolucionado con el uso creativo de Internet, permitiendo a los tratantes expandir sus operaciones por todo el mundo. Utilizan las redes sociales para buscar posibles víctimas, creando perfiles falsos e infiltrándose en grupos para identificar a personas en situación de desesperación, ocultando sus verdaderas intenciones. Las nuevas tecnologías e Internet son elementos facilitadores en el delito de trata, permitiendo actuar a tratantes y grupos criminales con mayor alcance, al asumir menores riesgos y mayores beneficios, y todo bajo el anonimato que otorgan los entornos digitales, lo que dificulta su persecución e imputación.

Durante el proceso de sometimiento de las potenciales víctimas, en su captación y explotación, así como en la publicidad de estas o sus servicios, el blanqueo de beneficios, e incluso en el control y coacción de las mismas, se destaca el uso de herramientas digitales como aplicaciones, redes sociales, plataformas, mensajería instantánea, videochat, video *streaming*, etc.

Según detalla la jurisprudencia, se acepta la comisión de la captación, así como otros tipos penales de delitos contra la libertad sexual, aceptando que el delito (incluida la captación en la trata de mujeres con fines de explotación sexual) «*puede ser cometido en el ciberespacio*»[199]. En este sentido, un ejemplo es el que se recoge en la STS núm. 301/2016, Sala 2ª, de lo Penal, de 12 de abril, Rec. 1229/2015, que confirma la condena por un delito de abuso sexual, que no se ve obstaculizada por el hecho de que no medie contacto físico entre agresor y víctima. La resolución establece que la afectación al bien jurídico de la indemnidad sexual de un menor puede producirse sin necesidad de contacto físico directo, dentro de un contexto de interacción sexual virtual. El Tribunal determina la existencia de un delito de abuso sexual sin necesidad de contacto físico:

> «Pero más allá de aquellos supuestos en los que la falta de contacto físico se produce en un contexto de proximidad entre agresor y víctima, las nuevas formas de comunicación introducen inéditos modelos de interrelación en los que la distancia geográfica deja paso a una cercanía virtual en la que la afectación del bien jurídico, no es que sea posible, sino que puede llegar a desarrollarse con un realismo hasta ahora inimaginable. El intercambio de imágenes de claro

[199] TAMARIT SUMALLA, J. M.; «Cibersexo transaccional: victimización en la intervención penal» *IDP: revista de Internet, derecho y política*, 2022, n.º 37, pp.2-4.

contenido sexual, obligando a un menor a enviar fotografías que atentaban contra su indemnidad sexual (ATS 1474/2014, 18 de septiembre), la obtención de grabaciones con inequívocos actos sexuales ejecutados por menores de edad (STS 864/2015, 10 de diciembre), la introducción anal y vaginal de objetos por parte de dos niñas, inducidas por su propia madre para su observación por un tercero a través de Internet (STS 786/2015, 4 de diciembre), son sólo algunos ejemplos bien recientes de resoluciones de esta Sala en las que hemos considerado que el ataque a la indemnidad sexual del menor de edad puede producirse sin esa contigüidad física que, hasta hace pocos años, era presupuesto indispensable para la tipicidad de conductas de agresiones o abusos sexuales a menores».

Esta forma de interacción a través de las redes sociales con finalidad de captar a la víctima se produce cada vez con más frecuencia, debido a que el uso del elemento tecnológico favorece la impunidad y el engaño a las víctimas. A modo de ejemplo, la Sentencia de la Sala de lo Civil y Penal del Tribunal Superior de Justicia de Cantabria núm. 21/23, de 21 de noviembre, confirma la pena impuesta a los autores de un delito de trata de mujeres con fines de explotación sexual, en concurso medial con un delito de prostitución coactiva. Como punto de partida, cabe destacar el contacto inicial entre acusada y víctima por medio de redes sociales, ofreciéndole un trabajo en España, eludiendo mencionar que se trataba de prostitución. La víctima mantuvo su relato de manera consistente sobre este hecho, que fue respaldado por las evidencias electrónicas (teléfonos móviles) y conversaciones que corroboraron la captación por medio de la plataforma en línea y la posterior coacción para ejercer la prostitución.

En los hechos probados, según se detalla en la resolución, se aprecia que el medio de captación se produce a través de redes sociales como mecanismo de engaño:

«Según los hechos probados, la encargada del piso, su hijo y otra chica, que ejercía la prostitución, "decidieron conseguir una chica joven en su país de origen, Colombia, con el fin de explotarla sexualmente y obtener un beneficio económico". Así las cosas, la mujer que ejercía la prostitución en el piso contactó a través de las redes sociales con una amiga de la infancia y, conociendo su situación de necesidad económica, le ocultó que iba a dedicarse a la prostitución y se ofreció a buscarle un trabajo en España. Además, se brindó a enviarle el billete de avión y dinero para el viaje y los primeros gastos, "logrando así, aprovechándose de su precariedad económica y de la confianza que le tenía, que viniera a España". Para ello, el hijo de la encargada sacó un billete de avión y se lo remitió por correo electrónico a la joven, que acudió al aeropuerto en Colombia donde un individuo que colaboraba con los acusados le entregó 900 dólares para posibilitar su paso por las fronteras como turista. Una vez en España, le esperaba otro hijo de la encargada, quien le reclamó el dinero que le habían entregado en su país de origen y la condujo a un vehículo que la llevó a Torrelavega. Allí fue recogida por el otro hijo, que la llevó a un piso de Santander, donde fue acogida por la que era su amiga y por otra chica, que también se prostituía. En el piso se presentó la encargada, que "le dijo que tenía que ejercer la prostitución hasta que abonara la deuda que había contraído con ella". Ante el temor que tenía y puesto que carecía de recurso alguno para solventar la deuda, hallándose en un país extranjero, sin dinero y sin contacto alguno familiar o social al que poder acudir y en su situación irregular, y ante las amenazas que la encargada le vertió relativas a que si no lo hacía matarían a su padre en Colombia, accedió a ello».

En los entornos virtuales, como en el marketing comercial, se utilizan diferentes técnicas en atención a quién va dirigida la estrategia digital, si a las potenciales víctimas o a los futuros clientes y, dependiendo de la finalidad de explotación a la que se dirija la misma. En este sentido, se utilizan técnicas de identificación de perfiles mediante algoritmos y se distribuyen mensajes mediante burbujas filtro y cajas eco. Los y las menores no son ajenos a estas estrategias. Por el contrario, dada su mayor vulnerabilidad, resulta más sencilla su captación y sometimiento, siendo que, además, sufren una mayor lesión precisamente por su condición de edad.

Todo esto no debe hacernos olvidar que el acceso a Internet se produce cada vez por personas más jóvenes, con un aumento del número de menores que comienzan a utilizar la red desde una edad temprana. Los niños, las niñas y adolescentes son blanco fácil de tratantes que los contactan a través de plataformas y redes sociales, aprovechando su vulnerabilidad y búsqueda de aceptación. La explotación sexual ha evolucionado. Ahora se lleva a cabo a través de tecnologías como videollamadas, sesiones en directo y la producción de material de abuso en línea. Los tratantes ya no necesitan movilizar a las víctimas a otros países, pueden realizar toda la operación desde la comodidad de su hogar, ampliando así las posibilidades de explotación en diferentes formas y lugares y a un mayor número de víctimas, con las dudas que se generan en torno a la posibilidad de incluir este tipo de conductas en el ámbito de aplicación del art. 177 bis[200].

En todo caso, factores como el alcance, la inmediatez, el anonimato o las posibilidades de acceso a grupos vulnerables como niños, niñas y adolescentes, definen el nuevo paradigma que suponen las nuevas tecnologías e Internet en la comisión de supuestos de explotación sexual de las personas, como un delito contra los derechos humanos.

Ante esta nueva realidad, resulta esencial que gobiernos, autoridades y organizaciones colaboren para identificar las nuevas formas de explotación en línea y desarrollen estrategias para prevenir y combatirlas en los entornos digitales, junto con el establecimiento de medidas adecuadas para que el uso de la tecnología no facilite la comisión de acciones de trata de seres humanos en ninguna de sus manifestaciones[201].

---

[200] De forma pionera en nuestro país, se ha considerado como víctima de trata a una mujer que trasladaba droga dentro de su cuerpo con la finalidad de explotación delictiva, lo que conduce a la aplicación de la eximente de responsabilidad penal por el delito cometido que se contempla en el propio precepto. Sobre esta cuestión se pronuncia VALLE MARISCAL DE GANTE, M. *«La sentencia de 2 de noviembre de 2021 del Tribunal Superior de Justicia de Cataluña: un importante paso hacia adelante en la protección de las víctimas de trata*» Diario La Ley n.º 9986, 11 de enero de 2022. Esta resolución ha quedado anulada por la STS núm. 960/23, de la Sala 2ª, de lo Penal, de 21 de diciembre, Rec. 7441/2021, lo que supone una pésima noticia para las víctimas de trata de seres humanos, ya que restringe la aplicación del «principio de no punición», que prevé la posibilidad de no imponer castigo a la víctima de trata por los delitos que se haya visto obligada a cometer como consecuencia de la situación de abuso y sometimiento que configura la trata de seres humanos. Este principio es una pieza clave en la protección a las víctimas de trata. El principio de no punición fue introducido en nuestro Código Penal en el año 2010, a través de la cláusula del artículo 177 bis 11. Tanto la sentencia de instancia como de apelación habían considerado víctima de delito de trata a la mujer a los efectos de aplicar esta cláusula del 177 bis 11. Sobre este tema se pronuncia MARTINEZ ESCAMILLA, M.; «La ligereza del Tribunal Supremo ante las víctimas de trata. Sentencia 960/2023 de la Sala Segunda del Tribunal Supremo, de 21 de diciembre», Crítica Penal y Poder, (Dossier «Migración y trata. Algunas sentencias relevantes»), 2024, n. 26.

[201] En este sentido, como ya se ha dicho, el Consejo de Ministros aprobó, en junio de 2024, un Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, donde, entre otras

8. LA PRUEBA DIGITAL

Debido al rápido avance tecnológico y al uso generalizado de dispositivos electrónicos o digitales en todos los aspectos de la vida, la cantidad de pruebas digitales disponibles ha aumentado considerablemente. Además, los criminales emplean cada vez más servicios y herramientas tecnológicas para organizar y cometer delitos de diversa índole. Las pruebas electrónicas se han convertido en fundamentales para luchar contra los ilícitos. La prueba se constituye a través de cualquier información relevante que se produce, guarda o transfiere con el empleo de dispositivos informáticos y que puede emplearse para demostrar un hecho en un juicio; eso es, se trata de información de importancia probatoria contenida en un medio informático o transmitida a través de este.

En el caso de las evidencias digitales, habría que diferenciar entre el hallazgo y posesión de los soportes de almacenamiento requisados e instrumentos de comunicación telemática (ordenadores, teléfonos móviles, *smarthphones*, tabletas, tarjetas de memoria, dispositivos USB, CD, DVD, MP3 o MP4, *routers*, etc.). Es decir, el material físico donde se escriben y almacenan los datos, que podría constituir una prueba en sí misma, esto es, como indicio en la existencia, autoría o circunstancias del hecho punible y, por otro lado, la información extraída y contenida en esos dispositivos electrónicos. De tal forma que, el contenido del dispositivo y el propio dispositivo serían considerados prueba en el proceso.

Por lo que hace a los datos, se puede distinguir entre *datos de abonados, datos de contenido* y *datos de tráfico*:

Los primeros son aquellos que se refieren a la suscripción de un servicio y proceden de la entidad suscriptora y están relacionados con la identidad del usuario, como son: la identificación del cliente, el nombre, la fecha de nacimiento, la dirección postal o de facturación, el número de teléfono, el correo electrónico e instante de activación/desactivación de la contratación o direcciones IP.

Los segundos son aquellos que se presentan en cualquier formato digital, como correos electrónicos, mensajes de texto o voz, imágenes, sonidos, fotografías y vídeos.

Los terceros son los relacionados con la prestación de un servicio ofrecido por proveedores de servicios en línea que permitan proporcionar información adicional o contextual, tales como el origen o el destino de una comunicación u otro tipo de interacción: la ubicación, fecha, hora, duración, ruta y conexión y desconexión, de relevancia como medios de convicción o vestigios del delito.

La rápida evolución de la tecnología y la creciente importancia de la evidencia digital en los casos judiciales plantean desafíos para el sistema judicial. En muchos casos, los jueces y letrados pueden carecer de 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. Los jueces y letrados pueden enfrentar dificultades para comprender los aspectos técnicos y forenses, lo que puede llevar a decisiones erróneas o a una falta de apreciación adecuada de la importancia de dicha evidencia en el

---

cuestiones, se trata de la necesidad de controlar el acceso de los menores a los contenidos pornográficos en la red, y la protección de los mismos frente a posibles ataques a su dignidad y libertad sexual.

caso[202]. A diferencia de lo que ocurre en la Fiscalía, que sí ha implementado salas especializadas de criminalidad informática, la judicatura no se ha especializado, por lo que sería conveniente que se realizaran formaciones específicas en esta materia.

Para abordar esta falta de especialización, es fundamental la capacitación y formación continua de todos los operadores jurídicos, así como de las Fuerzas y Cuerpos de Seguridad en temas digitales y tecnológicos, que permitan la adquisición de conocimientos básicos sobre informática forense, análisis de evidencia digital y aspectos legales relacionados con la tecnología.

8.1. *Características de la prueba digital*

La prueba digital presenta características propias en comparación con la prueba tradicional. Sus características son:

1. Intangibilidad	No se puede percibir físicamente a simple vista. Para su extracción y análisis, se requiere de procesos informáticos especializados y herramientas forenses digitales.
2. Replicabilidad	Puede ser fácilmente copiada o reproducida indefinidamente sin que se altere su contenido original. Esto plantea el desafío de distinguir entre el original y las copias, así como de garantizar la integridad de la prueba
3. Manipulabilidad	Es fácilmente manipulable, lo que implica que puede ser modificada o alterada sin dejar rastro aparente. Esto exige la implementación de medidas de seguridad y protocolos para garantizar la autenticidad e integridad de la prueba.
4. Volatilidad	Puede ser eliminada, destruida o modificada con facilidad. Esto puede dificultar su obtención o preservación, especialmente si no se toman las medidas adecuadas para su conservación y protección.

A pesar de la simplicidad con la que puede ser eliminado un rastro digital, hay que indicar que, con las técnicas forenses y herramientas adecuadas, podría localizarse la huella. Es decir, el vestigio que se deja cada vez que alguien interactúa en línea (registros de actividad, direcciones IP, datos de navegación, comunicaciones electrónicas, patrones de comportamiento, etcétera), o secuencia de eventos que llevaron a la comisión del delito, puede proporcionar información importante que consiga vincular a los sospechosos con los delitos cometidos y proporcionar pruebas para el enjuiciamiento. Por tanto, este rastro digital desempeña un papel crucial en la investigación y persecución del delito.

Dada la naturaleza de la prueba digital y sus características específicas, es fundamental contar con expertos en informática forense y técnicas de extracción, análisis y preservación de evidencia digital.

---

[202] Aquí hay diversas formaciones que se ofrecen para la enseñanza y la participación también en las jornadas sobre ciberseguridad. Disponible en: https://www.fiscal.es/-/criminalidad-informatica

8.2. *Fases en la obtención de la prueba digital*

La obtención de pruebas digitales de distintos tipos de delitos, no sólo los cibernéticos, es crucial para su investigación, por ejemplo, en un supuesto de quebrantamiento de condena por incumplimiento del deber de comunicación con la víctima con evidencia en mensajes de *WhatsApp.*

Es esencial tomar medidas para proteger la autenticidad e integridad de las fuentes de información digital durante su obtención, incorporación y el desarrollo de procesos judiciales, ya que los datos de los dispositivos electrónicos pueden ser alterados, eliminados o reemplazados con facilidad. Por ello, resulta crucial mantener correctamente la cadena de custodia para evitar la anulación de la prueba y la contaminación del resto de evidencias por la teoría del árbol envenenado[203].

En la investigación penal es cada vez más común incautar equipos informáticos y dispositivos de almacenamiento de datos. En este contexto, es crucial determinar los medios de prueba apropiados para incorporarlos al proceso legal. Por lo tanto, podemos concluir que, en el proceso penal, lo importante es el contenido de la información encontrada en estos dispositivos, no el dispositivo en sí. A diferencia de los delitos convencionales, la información pertinente y el proceso de ataque del infractor están presentes en sistemas informáticos.

La obtención de la prueba digital tiene distintas fases: acceso al contenido y diligencias de investigación, incorporación de la información al proceso judicial y valoración de datos.

8.2.1. Acceso al contenido y diligencias de investigación

Las primeras actuaciones en cualquier proceso son de suma importancia. La obtención de la prueba puede realizarse de diferentes maneras. Por un lado, las partes involucradas pueden aportarla al proceso. Por otro lado, en el contexto de una investigación, la Policía judicial puede obtenerla y luego presentarla en el proceso. Sin embargo, en este último escenario, es necesario contar con una autorización judicial si existe la posibilidad de que se vulneren los derechos fundamentales del sujeto bajo investigación.

La mera incorporación de la evidencia digital al procedimiento en relación con la posible comisión de un delito, ya sea en forma impresa en papel o en un dispositivo de almacenamiento como un *pendrive* o memoria USB, mediante capturas de pantalla o volcado de chat o mensajes, o grabación si son audios o vídeos, no garantiza por sí sola la autenticidad, integridad, contenido, ausencia de manipulación o autoría de la prueba. Cuando se presenta una prueba digital por un particular verificada ante un Notario o Notaria o Letrado o Letrada de la Administración de Justicia, su valor probatorio puede seguir siendo cuestionado, debido a que estos profesionales no tienen los conocimientos técnicos ni

---

[203] Esta doctrina se consolida en España, tras la STC núm. 114/1984, de 21 de diciembre, Rec. 167-1984, que estableció que no debían tenerse en cuenta las pruebas obtenidas cuando se habían vulnerado derechos fundamentales como la libertad y la intimidad. Igualmente, de la citada sentencia se deriva el artículo 11.1 de la Ley Orgánica del Poder Judicial de 1985, donde se dice que

> «*en todo tipo de procedimiento se respetarán las reglas de la buena fe, y no surtirán efecto las pruebas obtenidas, directa o indirectamente, violentando los derechos o libertades fundamentales*».

las herramientas necesarias para realizar un análisis forense digital exhaustivo que permita asegurar la integridad y fiabilidad de la prueba, ya que la simple impresión en papel o la copia en un dispositivo no acredita que la prueba no haya podido ser manipulada.

En este caso, el papel de las personas que ejercen la función pública se limita a constatar que no existen diferencias aparentes entre el texto o audio original y la copia aportada al proceso. Sin embargo, esto no implica que se pueda garantizar el origen de la evidencia, su autenticidad o su contenido sin ninguna duda.

De igual modo, los terceros de confianza pueden intervenir para dar fe de la fiabilidad de la prueba. Estos intervinientes podríamos definirlos como aquellos sistemas informáticos o empresas que implementan tecnologías como la firma electrónica y el sellado de tiempo para certificar y almacenar documentos electrónicos que atestiguan hechos o actos jurídicamente relevantes en el mundo virtual. Estos sistemas cumplen con estándares de seguridad y otorgan a los documentos el valor probatorio necesario para poder ser utilizados como prueba instrumental en un proceso judicial. Los terceros de confianza están recogidos en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

En esta fase inicial de investigación, debemos mencionar la llevada a cabo por La Policía judicial. En concreto, en la Policía nacional, corresponde a la Brigada de Investigación Tecnológica, y en la Guardia Civil, al Grupo de Delitos Telemáticos. Las medidas de investigación tecnológica fueron introducidas por la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica. Estas medidas están recogidas en el Título VII, del Libro II de la Ley de Enjuiciamiento Criminal, concretamente en los capítulos IV a X.

Hasta esta modificación de 2015, nuestra legislación carecía de una regulación específica en relación con las investigaciones tecnológicas, y las decisiones judiciales suplían esta falta de normativa. Los tribunales advirtieron que la obtención de la prueba podría afectar a la privacidad y derechos fundamentales del acusado, tales como el derecho a la intimidad o el secreto de las comunicaciones. Asimismo, se debe tener presente el derecho a la protección de datos personales, el derecho al propio entorno digital, el derecho a la inviolabilidad del domicilio y el derecho a la propia imagen. Estos derechos exigen que las pruebas se obtengan respetando las garantías constitucionales más rigurosas pues, de lo contrario, podrían ser excluidas, afectadas de nulidad.

En este punto, queremos reseñar que tanto el Tribunal Europeo de Derechos Humanos ya en la mencionada sentencia de 2008[204], como el Tribunal Supremo de Estado Unidos en 2014[205], destacaron la importancia de contar con un control judicial frente a la vulneración grave de la privacidad que podría suponer un análisis sin límites de un teléfono inteligente. Por lo tanto, es ilícita la prueba obtenida produciendo vulneración de derechos fundamentales.

---

[204] STEDH de 22 de mayo de 2008, Caso Iliya Stefanov *vs.* Bulgaria.

[205] Tribunal Supremo de Estados Unidos, Sentencia 25 junio 2014, (casos acumulados Riley contra California y Estados Unidos contra Brima Wurie-573 U.S.-2014).

8.2.2. Policía judicial: medidas de investigación tecnológica

Las diligencias de investigación podrán ser adoptadas bajo autorización judicial, siempre y cuando se cumpla con los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida. El juez o la jueza acordará de oficio o a petición del Ministerio Fiscal o de la Policía judicial las medidas de averiguación contenidas en la Ley de Enjuiciamiento Criminal (LECrim). Con carácter general, el juez o la jueza de instrucción autorizará o denegará la medida en un plazo máximo de veinticuatro horas mediante auto motivado, ya que la limitación de los derechos del afectado deberá alcanzar exclusivamente a lo estrictamente necesario para conseguir los fines de la investigación. En los casos de urgencia en que se aprecie un interés constitucional legítimo que haga imprescindible la medida la Policía judicial puede tener acceso al contenido de los dispositivos. En este caso, lo pondrá en conocimiento inmediato del juez, que en un plazo máximo de 72 horas ratificará el acceso argumentando el motivo de la urgencia. (artículo 588 sexies c apartado 4 LECrim).

Por consiguiente, ante las especialidades de la prueba digital y su facilidad de manipulación y volatilidad, la LECrim contempla medidas a tener en cuenta para su obtención, aseguramiento y preservación desde el momento en que son recolectadas hasta su presentación en un proceso legal, evitando cualquier alteración o contaminación, que son: la entrada y registro; los registros en remoto; y la figura del agente encubierto.

De acuerdo con la jurisprudencia, la entrada y registro en un domicilio sólo se considera legítima si se realiza con el consentimiento del propietario o en caso de flagrante delito. Por lo tanto, si no se cumplen estos dos requerimientos, será necesario contar con una autorización judicial que justifique la necesidad de llevar a cabo dicha medida.

En otras palabras, aunque la autorización judicial permite confiscar los dispositivos, se requiere una justificación judicial adicional y separada para acceder a la información contenida en ellos. Esta justificación puede ser incluida en la misma orden de entrada y registro o en una orden separada.

Cuando el juez de instrucción emite una autorización de entrada y registro domiciliario, esta autorización se limita exclusivamente a confiscar los dispositivos electrónicos y sin posibilidad de acceso a su contenido. En aquellos casos en los que se pueda prever la existencia de un contenido ilícito en esos dispositivos de almacenamiento masivo de información (por ejemplo, pornografía infantil), el juez puede extender la autorización de acceso al contenido en ese mismo auto o posteriormente, puesto que, de no ser así, se podrían vulnerar los derechos al secreto de las comunicaciones e intimidad y no sólo la inviolabilidad del domicilio.

Aquellos dispositivos incautados fuera de un registro domiciliario, como por ejemplo a consecuencia de una detección policial, precisan bien de la autorización de la persona propietaria, bien de autorización judicial para el registro de su contenido, pero no para su incautación.

En cuanto a los registros en remoto, como diligencia de investigación y siempre con autorización previa, pretenden evitar la pérdida o destrucción de información y se orientan a la búsqueda de indicios o vestigios de la comisión del ilícito penal. Hay dos características fundamentales que distinguen las medidas de investigación tecnológica remotas de las medidas de investigación directas:

la clandestinidad y la naturaleza dinámica del registro. Se utilizan cuando se requiere de una actuación rápida, necesaria y excepcional. Permiten la interceptación de comunicaciones en tiempo real y su seguimiento durante el tiempo que dure la medida. En este caso, no será posible llevar a cabo un registro policial que posteriormente sea validado por el Juez, ni en situaciones de urgencia, ni cuando se quiera ampliar el registro a otros sistemas, como se hacía con los registros directos.

Estos registros remotos sólo se contemplan para investigar una serie de delitos, contenidos en el artículo 588 a) *septies* de la Ley de Enjuiciamiento Criminal, entre otros, aquellos cometidos contra menores o personas con capacidad modificada judicialmente y los delitos cometidos a través de instrumentos informáticos o de cualquier otra tecnología de la información o telecomunicación o servicio de comunicación.

Con autorización judicial existen dos maneras de llevar a cabo registros remotos: a través de la utilización de las contraseñas del investigado, obtenidas como resultado de la investigación policial, o mediante la instalación de herramientas que permitan realizar exámenes en remoto del contenido de su ordenador, sin que el propietario o usuario tenga conocimiento, aunque esto último presenta la dificultad de su instalación.

El agente encubierto en investigaciones policiales se utiliza para infiltrarse en línea en grupos delictivos o en actividades ilegales. Este tipo de agente actúa de manera incógnita, es decir, ocultando su verdadera identidad y propósito para recopilar información sobre actividades delictivas o criminales. Utiliza diferentes técnicas para recopilar información, como el *hackeo* ético, el uso de redes sociales falsas o la infiltración en grupos en línea. Su objetivo es recabar pruebas que puedan ser utilizadas en un caso judicial y desmantelar organizaciones criminales o prevenir actos delictivos. Es importante mencionar que el uso de agentes encubiertos informáticos está sujeto a autorización judicial mediante resolución motivada y es aplicable para los delitos contenidos en los artículos 282 bis 4 y 579.1 LECrim.

A mayor abundamiento, se debe mencionar que todos los proveedores de servicios de telecomunicaciones, de acceso a redes de comunicación o servicios de la sociedad de la información están obligados a brindar la asistencia necesaria y colaborar con el juez, el fiscal y los agentes de la Policía judicial designados para llevar a cabo las medidas de intervención de las telecomunicaciones, a fin de garantizar el cumplimiento de las órdenes judiciales, que pueden tener entre otras finalidades, la identificación y localización del terminal, la identificación del infractor o de números de teléfono.

Con el objetivo de garantizar la integridad de la prueba que pueda resultar de los datos almacenados en un instrumento digital se adoptarán una serie de cautelas y garantías:

1. *Clonado de información*, que puede realizarse en el mismo lugar en que se encuentra la evidencia digital o en un momento posterior. Para realizar la copia, no sería necesaria la intervención del Letrado o Letrada de la Administración de Justicia (LAJ), pero sí aconsejable. Es imprescindible preservar la cadena de custodia en el volcado o clonado de la información contenida en los dispositivos. Como pasos principales para ello destacan: la identificación y recolección de las evidencias digitales (dispositivos electrónicos, medios de almacenamiento, registro de actividad, archivos, correos electrónicos, etcétera); etiquetado, embalaje y registro, las evidencias se marcan de manera única, incluyendo su descripción, ubicación, fecha y hora de recolección y

personas involucradas en su manejo. Este marcado *(hash* criptográfico)[206] permite documentar el historial de actividades que se han llevado a cabo durante el proceso, y de los hallazgos encontrados de modo que posibilite la reconstrucción del hecho después del transcurso del tiempo desde que fue analizado. Es decir, la imagen obtenida con la copia será idéntica a la original.

Sin embargo, en casos en los que el dispositivo no sea incautado y permanezca en posesión del investigado, se requerirá realizar dos copias. La primera copia servirá para asegurar y garantizar el contenido del dispositivo en un momento específico, mientras que la segunda copia será utilizada para llevar a cabo los análisis necesarios exigidos por la investigación. De esta manera, se garantiza la integridad de la primera copia al ser sellada y custodiada por el/la LAJ, quien la utilizará como muestra de contraste.

Los volcados realizados por la Policía judicial no contarán con las garantías otorgadas por la presencia de un/a LAJ. Sin embargo, podrán ser presentados como evidencia en el juicio siempre que vayan acompañados de la declaración de los/las agentes policiales que realizaron el volcado. Sin perjuicio de la posible impugnación que de dicha prueba pudiera hacer la defensa.

Autorización judicial para el *cambio de claves de acceso*, impidiendo que se pudiera acceder o modificar posteriormente a los datos por parte de cualquier persona (art. 326 LECrim).

2. *Intervención del Letrado o Letrada de la Administración de Justicia*. Es necesario documentar los registros realizados, donde el/la LAJ es responsable de levantar un acta detallando las operaciones realizadas y las personas que participaron en el registro. En la documentación se debe incluir el IMEI (identificador único que tiene cada teléfono móvil) del dispositivo, el número de serie del disco duro y los precintos del material electrónico para asegurar la cadena de custodia. Su presencia es indispensable durante la entrada y registro del lugar cerrado en el que se encuentre el dispositivo, siendo prescindible en el proceso de volcado de datos, al no ser experto en la materia. De este modo, habría que adoptar algún tipo de garantía en aras a la preservación de la prueba en el momento del volcado, ya que el/la LAJ carece de la formación necesaria y especializada a nivel tecnológico.

8.2.3. Incorporación de la información al proceso judicial

El hecho electrónico puede ser introducido en el proceso mediante un documento físico, o bien a través de medios de prueba convencionales como interrogatorios, testimonios, peritajes o reconocimiento judicial, mediante el cual el juez o la jueza puede acceder directamente al contenido del soporte electrónico para visualizarlo o escucharlo.

En el ámbito del proceso penal, las pruebas informáticas están sujetas a las mismas reglas de admisibilidad que las establecidas en la LECrim para las pruebas analógicas o tradicionales. La validez

---

[206] *Hash* criptográfico: algoritmo único e irrepetible. Cualquier acceso no autorizado a la prueba generaría una alteración en ese número de identificador, permitiendo diferenciar entre original y copia.

de un documento electrónico depende de su autenticidad y seguridad, al igual que cualquier otra prueba. La credibilidad de un documento electrónico aumenta en la medida en que sea más seguro y auténtico.

Es frecuente en la práctica aportar a la causa conversaciones entre víctima e investigado, siendo las mismas cotejadas por el/la LAJ. En la mayoría de las ocasiones, esta prueba no es impugnada de contrario, pero debemos señalar que, en el caso de que la prueba sea impugnada, debe ser la parte que pretende aprovechar su idoneidad la que identifique el verdadero origen de la comunicación. Así se expresa en la STS núm. 300/2015, Sala 2ª, de lo Penal, de 19 de mayo, Rec. 2387/2014, en el sentido siguiente:

> «(…) Y es que la prueba de una comunicación bidireccional mediante cualquiera de los múltiples sistemas de mensajería instantánea debe ser abordada con todas las cautelas. La posibilidad de una manipulación de los archivos digitales mediante los que se materializa ese intercambio de ideas, forma parte de la realidad de las cosas. El anonimato que autorizan tales sistemas y la libre creación de cuentas con una identidad fingida, hacen perfectamente posible aparentar una comunicación en la que un único usuario se relaciona consigo mismo. De ahí que la impugnación de la autenticidad de cualquiera de esas conversaciones, cuando son aportadas a la causa mediante archivos de impresión, desplaza la carga de la prueba hacia quien pretende aprovechar su idoneidad probatoria. Será indispensable en tal caso la práctica de una prueba pericial que identifique el verdadero origen de esa comunicación, la identidad de los interlocutores y, en fin, la integridad de su contenido».

Por ende, para garantizar la validez y la eficacia legal de la prueba digital en un procedimiento judicial, es conveniente aportar un informe pericial informático emitido por expertos informáticos, profesionales capacitados para llevar a cabo un análisis técnico avanzado que permita detectar posibles manipulaciones, origen, autenticidad y autoría, que examinará la evidencia digital presentada, ya sean archivos, mensajes, registros de actividad, metadatos, entre otros. Este informe pericial podrá ser emitido por un/a profesional privado/a o público/a del juzgado.

De igual manera, es recomendable que el perito informático sea emplazado a declarar a la mayor brevedad posible, principalmente en fase de instrucción, para evitar impugnaciones o inadmisiones posteriores en fase de juicio oral. En esta citación, se encargará de ratificar el informe emitido, facilitando la posibilidad de realizarle cualquier cuestión o petición de aclaración con respecto a su texto, asegurando el principio de contradicción.

El informe pericial informático tiene como finalidad respaldar o refutar las afirmaciones o argumentos presentados por las partes en el proceso judicial, otorgar confiabilidad de la evidencia digital y ayudar a la judicatura y a los/as profesionales de la abogacía a comprender los aspectos técnicos relevantes del caso, ya que proporciona detalles técnicos, resultados del análisis y conclusiones basadas en los hallazgos obtenidos durante el examen forense digital. El informe debe ser claro, objetivo y estar sustentado en principios científicos y normativas legales aplicables en relación a su licitud, pertinencia y observancia de todas las garantías legales para su obtención. El informe emitido contendrá entre otros, datos relativos a contenidos, información eliminada, cronología de los hechos, identificación de dispositivos e interpretación de referencias, así como detección del rastro existente en portátiles, servidores, dispositivos móviles.

La aportación al proceso de conversaciones entre víctima e investigado requiere, además, la transcripción de las mismas, no siendo suficientes los pantallazos, así lo manifiesta la reiterada jurisprudencia, entre la que se puede citar, la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Galicia núm. 556/2016, de 28 de enero, que distingue cuatro supuestos para aceptar un documento o mensaje instantáneo:

> «(…) no sólo la copia en papel de la impresión de pantalla o, como se denomina usualmente, "pantallazos" –que es lo único se cumple por el actor–, sino una transcripción de la conversación y la comprobación de que ésta se corresponde con el teléfono y con el número correspondientes. Esto podría haber conseguido a través de la aportación del propio móvil del Sr….y solicitando que, dando fe pública, el LAJ levante acta de su contenido, con transcripción de los mensajes recibidos en el terminal y que éste se corresponde con el teléfono y con el número correspondientes, o, incluso, mediante la aportación de un acta notarial sobre los mismos extremos.
>
> *Apurando nuestras consideraciones sobre la prueba de mensajería instantánea y con fines esclarecedores, para que aceptemos como documento una conversación o mensaje de este tipo (algo diferente a su valor probatorio) podríamos establecer cuatro supuestos: (a) cuando la parte interlocutora de la conversación no impugna la conversación, (b) cuando reconoce expresamente dicha conversación y su contenido, (c) cuando se compruebe su realidad mediante el cotejo con el otro terminal implicado (exhibición), o finalmente, (d) cuando se practique una prueba pericial que acredite la autenticidad y envío de la conversación, para un supuesto diferente de los anteriores».*

En el caso de grabaciones de conversaciones o de notas de voz intercambiadas entre las partes, deben ser aportadas no solamente en formato electrónico de modo que se puedan reproducir en el acto de la vista, sino que también deben ser igualmente transcritas para su cotejo.

Por lo demás, toda esta prueba debe ser valorada como cualquier otra en su conjunto. En este sentido, la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid, núm. 83/2019, de 25 de enero, sostiene:

> «Por lo expuesto, los correos electrónicos pueden ser utilizados para elaborar el relato fáctico como un "elemento de convicción", al ser reiterado el criterio jurisprudencial que declara que "el documento privado no reconocido legalmente no carece de valor probatorio, lo que supondría dejar al arbitrio de una parte la eficacia probatoria del documento, y puede valorarse mediante su apreciación conjunta con otros elementos de juicio, pues en definitiva los documentos privados, aún impugnados, poseen un valor probatorio deducido de las circunstancias del debate"».

8.2.4. Valoración de datos

Las pruebas digitales serán valoradas conforme a las reglas de la sana crítica según establece el artículo 382.3 de la Ley de Enjuiciamiento Civil y, asimismo, a lo dispuesto en su artículo 326, en atención a la fuerza probatoria de los documentos privados. En este último caso, si no existe impugnación de contrario, su valor probatorio es igual a los documentos públicos.

Cuando únicamente se cuenta con la prueba digital y su autenticidad es impugnada por la parte contraria, se requiere la realización de una pericial informática. Sin embargo, si la prueba es impugnada,

pero no tenemos ese dictamen pericial que indica su autenticidad, pero tampoco se prueba que sea una evidencia falsa o manipulada, esta se valorará con otros indicios.

9. PROBLEMAS TRANSFRONTERIZOS. COOPERACIÓN INTERNACIONAL

De acuerdo con el Informe de Impacto que acompaña a la Propuesta de Reglamento E-Evidencia[207], más de la mitad de todas las investigaciones actuales implican una solicitud transfronteriza de acceso a pruebas electrónicas. En alrededor del 85 %, se requieren datos digitales y es preciso requerir pruebas a proveedores de servicios en línea con sede en otra jurisdicción en dos tercios de las investigaciones. En el período comprendido entre 2013 y 2016, el número de peticiones a los principales proveedores de servicios *online* creció un 70 %. Según señala DELGADO MARTÍN:

> «a menudo concurre una insuficiencia de los ordenamientos nacionales, así como diferencias entre los mismos; así como un diferente tratamiento legal de la retención y acceso a los datos en los diferentes países, o incluso una falta de legislación nacional que lo regule. La ausencia de instrumentos normativos internacionales adecuados contribuye a dificultar la utilización de los datos en poder de proveedores para la investigación y prueba de delitos»[208].

Por ende, el carácter transfronterizo y la ausencia de límites territoriales en la perpetración de delitos cibernéticos permite a los ciberdelincuentes valerse de esta característica para perpetrar el ilícito con cierta impunidad.

Por tanto, la obtención de pruebas electrónicas se enfrenta al desafío del acceso transfronterizo. Las autoridades se encuentran con dificultades debido a que los datos de las personas usuarias de los proveedores de servicios en línea a menudo se encuentran almacenados en servidores ubicados en diferentes países dentro y fuera de la Unión Europea. Esto incrementa la complejidad y prolonga el proceso para que las autoridades puedan recopilar dichas pruebas electrónicas y tiene efectos negativos para el estado de derecho y las obligaciones de los gobiernos de proteger a las personas en el ciberespacio.

En atención a la facilidad con la que la prueba electrónica puede ser eliminada, modificada o destruida, el acceso convencional a la evidencia digital en posesión de proveedores ubicados fuera del territorio nacional a través de una comisión rogatoria a menudo resulta ineficaz. Esto se debe a que los indicios

---

[207] COMISIÓN EUROPEA. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings,* 2018. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN

[208] DELGADO MARTÍN, J.; «Prueba Digital Internacional. El Reglamento E-Evidence», *Diario La Ley, n.º 76,* 2023. Disponible en: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAE-VQwW6DMAz9muY4QaGaesilwIGJdtCxaTtVJlgQKUtQnHTj7-eu0mbJlvVsP73nAAPJPBOgQgRTOiV3t15fsYfhN-nB-RH9YZSKCC2DOSDLN9rmg2X2d4KonCNrZA3jZ-4hCj8eme0Ejj2hj67VVegGTbi9pwrNRln3CkT3mu30mrui-Jj-WbntAGFLOe5oYz3LmASFMJAWT5XPQfbbXZ5mW_yYbqncvTK5dTJQjBq7mFCWWjKQArjCbA6Kiviweg5V-sowztMhAUYtOOfVmogWjV3Ef16h8w_UI-y6ZhCwLKY9ewMO__dWRzxn-InS65tAd5FYr_JD0DH_DxKAQAAWKE

pueden haber desaparecido, debido al largo tiempo que se requiere para obtenerlos a través de este método de acceso. Asimismo, existe la posibilidad de que la policía o la autoridad judicial del país puedan realizar una solicitud directa a los proveedores de servicios, quienes pueden optar por entregar la evidencia voluntariamente en función de su propia política interna, la cual varía en cada caso.

En relación con la mejora en el acceso transfronterizo a las pruebas electrónicas, en 2019 la Comisión Europea, por mandato del Consejo, propuso iniciar negociaciones internacionales para favorecer la localización de los delincuentes y simplificar los mecanismos de accesibilidad a las pruebas electrónicas. La Comisión entabló dos vías de negociación: una con Estados Unidos, que se encuentra en curso, y otra para la elaboración del ya mencionado Segundo Protocolo Adicional al Convenio de Budapest.

Un acuerdo entre EE. UU. y la UE establecería un ámbito de trabajo que incluiría una colaboración directa con los proveedores de servicios. Esto agilizaría el acceso a pruebas electrónicas, al reducir el tiempo de entrega de datos solicitados de un promedio de diez meses a tan sólo diez días. Además, se implementarían sólidas medidas de protección de los derechos fundamentales. 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 lo que respecta Convenio de Budapest, su Segundo Protocolo Adicional tiene como objetivo fortalecer la cooperación entre autoridades de los diferentes países en la lucha contra la ciberdelincuencia, así como garantizar una eficaz obtención y revelación de las pruebas electrónicas mediante la adopción de instrumentos adicionales, que promoverán una asistencia mutua más eficaz. Las medidas adoptadas serán acordes al respeto del estado de derecho y a las salvaguardas de la protección de datos y buscarán habilitar mecanismos que faciliten el auxilio directo entre proveedores y entidades que procuran servicio en otro Estado parte. No obstante, este código de actuación no ahonda en temas como la interceptación de comunicaciones en tiempo real, sino que esencialmente se refiere al acceso a datos almacenados. Por lo tanto, habrá que definir qué autoridades son las competentes en cada caso, tanto para cursar la solicitud transnacional como para la recepción de las que remitan otros países, lo que incluirá posiblemente alguna reorganización interna.

En principio, no se ve afectado el régimen interno de cada país, sino la forma en que nos vamos a relacionar con los demás. Esto no requerirá de una reforma legislativa importante porque, de hecho, las medidas de investigación que contempla la Convención se incorporaron en el ordenamiento español desde la reforma operada por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal (LECrim). Por ejemplo, ya podemos solicitar directamente a *Google* información sobre un dato de abonado por la vía del artículo 588 Ter m) de la LECrim. Ahora se trata de ver cómo adaptamos esas herramientas con las que ya contamos a las exigencias del Protocolo, para poderlas aplicar en el ámbito internacional.

Asimismo, el Segundo Protocolo establece procedimientos simplificados para la asistencia judicial mutua de emergencia, lo que permite una respuesta más rápida y eficiente en situaciones urgentes, en las que exista un riesgo significativo e inminente para la vida o la seguridad de cualquier persona física, con la posibilidad de reclamar la información directamente a los proveedores de servicios de

comunicaciones electrónicas y en línea, agilizando el proceso y evitando demoras innecesarias. Este Protocolo tiene un alcance global, ya que ha sido firmado por 34 países, incluyendo a 18 miembros de la Unión Europea. Su implementación complementará el marco interno de la Unión Europea para el acceso a las pruebas electrónicas, acordado entre el Consejo de la Unión Europea y el Parlamento Europeo y está en proceso de ser formalmente adoptado.

El paquete de medidas simplificará y acelerará el proceso de obtención de pruebas electrónicas por parte de las autoridades policiales y judiciales, lo que les permitirá investigar y enjuiciar a los delincuentes de manera más eficiente. En este sentido, recientemente, el Parlamento Europeo y el Consejo han dictado el Reglamento (UE) 2023/1543, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales, y la Directiva (UE) 2023/1544, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales, ambas decisiones de 12 de julio de 2023.

9.1. *Reglamento (UE) 2023/1543 sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales*

El objetivo de este Reglamento es implementar un mecanismo alternativo a los actuales instrumentos de cooperación internacional y asistencia judicial. Se centra en abordar, de manera específica, los desafíos derivados de la naturaleza volátil de las pruebas electrónicas y su falta de ubicación establecida. Este Reglamento establece nuevos procedimientos que permiten un acceso transfronterizo rápido, eficiente y efectivo a estas pruebas.

Igualmente, establece la creación de órdenes europeas de producción y conservación, las cuales pueden ser emitidas por las autoridades judiciales con el objetivo de obtener o preservar pruebas electrónicas, como direcciones IP, fecha y hora de conexión, correos electrónicos, mensajes de texto o mensajes en aplicaciones, así como información para identificar al autor (nombre, dirección, teléfono, correo electrónico etcétera).

1. Las órdenes de producción[209] permiten a la autoridad judicial de un Estado miembro obtener directamente evidencias digitales del proveedor de servicios o su representante legal en otro Estado miembro. Sin embargo, estas órdenes sólo pueden ser solicitadas para delitos punibles en el país emisor, con una pena máxima de, al menos, tres años de privación de libertad, siempre que se hayan cometido total o parcialmente a través de un sistema de información, o para delitos específicos relacionados con la ciberdelincuencia, la pornografía infantil, la falsificación de medios de pago distintos al efectivo o el terrorismo. Es obligatorio que se responda a una

[209] UE. Reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal, 17 de abril de 2018. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018PC0225&from=CS

orden de entrega en un plazo de diez días, aunque, en casos de emergencia, este plazo puede reducirse a seis horas. Los proveedores de servicios podrán ser sancionados, si no cumplen con estas órdenes, con multas monetarias que podrán alcanzar el 2 % del total de los ingresos anuales de la empresa a nivel global del año anterior.

2. Las órdenes de conservación impedirán que los proveedores de servicios destruyan las evidencias electrónicas de los datos almacenados, sin que permitan la interceptación de transmisiones en tiempo real. El proveedor de servicios deberá conservar los datos solicitados durante un máximo de 60 días, a menos que la autoridad emisora le informe de que ha puesto en marcha el procedimiento para emitir una solicitud posterior de entrega, en cuyo caso, la conservación deberá mantenerse. En caso de que un proveedor de servicios esté supeditado a un conflicto de leyes, se prevé un procedimiento específico. Se crea un sistema descentralizado de comunicaciones entre las distintas autoridades y los proveedores de servicios con carácter seguro y confiable que certifique la autenticidad.

9.2. *Directiva (UE) 2023/1544, por la que se establecen normas armonizadas para la designación de establecimientos designados y de representantes legales a efectos de recabar pruebas electrónicas en procesos penales*

Esta Directiva es la herramienta fundamental en la implementación del Reglamento, ya que instaura normas aplicables al nombramiento de los representantes legales de los proveedores de servicios o a la designación de sus establecimientos, responsables de aceptar y contestar a estas órdenes. En definitiva, los proveedores de servicios no instaurados en la Unión Europea, pero que prestan sus servicios en ella, deberán designar un representante legal, que estará a cargo de recibir, ejecutar y asegurar el cumplimiento de las decisiones y órdenes.

Por tanto, en los delitos cometidos por medio de Internet, la determinación de la competencia territorial puede ser más compleja debido a la falta de un lugar físico concreto, lo que deriva del carácter descentralizado del ciberespacio. Conforme al artículo 22.5 del Convenio sobre el Cibercrimen, es competente para la investigación el Estado que esté en mejores condiciones para ejercer la persecución del delito. El criterio de la eficacia de la instrucción permite atribuir la competencia al órgano judicial que se encuentre en mejores condiciones de abordar la persecución del delito y, para ello, es absolutamente preciso, lejos del automatismo que genera el principio de territorialidad, valorar elementos como la ubicación o residencia de los investigados, lugar donde se urdió el plan criminal, lugar donde se encuentren pruebas o evidencias del delito o, incluso, donde se haya desarrollado la estructura criminal puesta al servicio de tales fines. En este sentido se pronuncia la STS núm. 871/2022, Sala 2ª, de lo Penal, de 7 de noviembre, Rec. 10258/2022, que dice:

> *«las tradicionales dificultades para la determinación del órgano jurisdiccional competente para la investigación y enjuiciamiento de un hecho delictivo, se multiplican en los casos de delincuencia cometida a través de Internet. La red facilita el anonimato, amplificando la intensidad de los efectos asociados a la ofensa del bien jurídico. Por su propia naturaleza, la comunicación telemática implica la existencia de una ruta zigzagueante, definida por los correspondientes nodos, que obliga a la modulación de las tradicionales categorías llamadas a la delimitación del lugar en el que el delito ha de estimarse cometido. (...) tal y*

como fue definido en nuestro Acuerdo del Pleno no Jurisdiccional de 3 de febrero de 2005, con arreglo al cual "el delito se comete en todas las jurisdicciones en la que se haya realizado algún elemento del tipo, en consecuencia, el Juez de cualquiera de ellas que primero haya iniciado las actuaciones procesales será en principio competente para la instrucción de la causa". No deja de ser significativo que el Convenio sobre el Cibercrimen, suscrito en Budapest el 23 de noviembre de 2001, incorpore como criterio de atribución jurisdiccional, en los casos en que varios Estados reivindiquen su propia jurisdicción para enjuiciar una determinada infracción, la solución favorable a aquel Estado que «esté en mejores condiciones para ejercer la persecución (art. 22.5)».

En este marco de cooperación jurídica internacional, España firma en 2019 el Tratado Relativo a la Transmisión Electrónica de Solicitudes de Cooperación Jurídica Internacional entre Autoridades Centrales, conocido como Tratado de Medellín, ratificado por nuestro país en 2021. Este cuerpo normativo está abierto a la adhesión por cualquier país del mundo. Implica fomentar la cooperación entre los países firmantes en temas como la ciberseguridad, la protección de datos, la lucha contra el cibercrimen, la gobernanza de Internet y la promoción de la innovación y el desarrollo tecnológico.

En términos de cooperación internacional, este tratado facilita el intercambio de información y buenas prácticas entre los países firmantes, lo que permite una mejor coordinación de esfuerzos en la lucha contra los delitos cibernéticos y una mayor eficacia en la protección de los sistemas de información y comunicación a nivel mundial. Además, el Tratado de Medellín contribuye a establecer un marco común de normas y principios en el ámbito digital, lo que favorece la interoperabilidad entre los distintos sistemas y facilita la cooperación transfronteriza en este ámbito. Es un acuerdo internacional que facilita la comunicación electrónica entre las autoridades centrales de diferentes países en el marco de la cooperación jurídica internacional. Al haber ratificado este tratado, las autoridades españolas pueden enviar y recibir solicitudes de cooperación judicial de forma electrónica con otras autoridades centrales de los países firmantes. Esto reduce los tiempos y los costos asociados a la comunicación por medios tradicionales como el correo postal. Además, la transmisión electrónica de solicitudes, mediante la utilización de una plataforma segura, que pertenece a la Red Iberoamericana de Cooperación Jurídica Internacional, garantiza la seguridad y la confidencialidad de la información, contribuyendo a una mayor eficacia en la lucha contra el crimen transnacional.

CONCLUSIONES Y PROPUESTAS

CONCLUSIONES

PRIMERA

El uso de dispositivos electrónicos y tecnologías de la información y de la comunicación (TIC) ha crecido exponencialmente, especialmente a raíz de la pandemia por COVID-19, que fue el catalizador definitivo para la adopción de las tecnologías digitales. Este fenómeno se ha visto impulsado por la proliferación de redes sociales, aplicaciones móviles y servicios de Internet que se han integrado profundamente en la vida cotidiana de las personas, transformado no sólo la comunicación personal, sino también la que se produce en el ámbito social, educativo y laboral. Al mismo tiempo, ha facilita la comisión de actos ilícitos, especialmente siendo las víctimas las mujeres y las personas menores de edad.

SEGUNDA

Hoy por hoy existen múltiples definiciones del término «violencia digital». La carencia de un concepto universal y único impide una normativa uniforme en cuanto a su naturaleza, tipología, características, así como su regulación penal.

TERCERA

Las cifras estadísticas de las distintas investigaciones expuestas evidencian que la violencia digital afecta mayoritariamente a mujeres y a niñas. Es una extensión de la violencia ejercida fuera de línea, basada en la estructura patriarcal y en los roles de género que, lejos de desaparecer, se reproducen en el mundo virtual. De la misma manera, los datos revelan que las personas menores de edad acceden en edades más tempranas a los contenidos para adultos, puesto que son nativos digitales familiarizados con una red que establece barreras de protección muy débiles y carecen de educación afectivo-sexual.

CUARTA

Las TIC constituyen una herramienta que se puede utilizar para facilitar el empoderamiento de las mujeres. Además, se han convertido en un medio para contribuir a la organización de la acción colectiva feminista y para visibilizar discursos de concienciación y reivindicación social a gran escala, así como para aumentar el poder de convocatoria, superando las limitaciones espaciales existentes en el ámbito analógico. Del mismo modo, han supuesto la creación de nuevas oportunidades para la educación, el empleo y la socialización.

QUINTA

El uso de la inteligencia artificial implica constatar la existencia de sesgos inherentes a los datos con los que se genera, lo que puede provocar decisiones discriminatorias o injustas. Además, para su aprendizaje requiere de la recopilación, análisis y almacenaje de grandes cantidades de datos

personales, lo que interfiere en nuestros derechos y garantías en relación con la privacidad y con la protección de información confidencial.

SEXTA

Las personas menores de edad son especialmente vulnerables a los riesgos de la interacción en línea. La exposición a contenido inapropiado, la facilidad de acceso a las redes sociales y la falta de supervisión adecuada contribuyen a la normalización de conductas inapropiadas y a la victimización. La falta de madurez y de juicio crítico en la infancia y en la adolescencia, junto con la insuficiente educación digital, les hace más susceptibles a ser explotadas y explotados por depredadores en línea, enfrentando riesgos como el *grooming*, el ciberacoso y la explotación sexual digital. La facilidad de acceso a las redes sociales y aplicaciones de mensajería ha permitido a los agresores ejercer un control invasivo y perpetrar diversas formas de ciberviolencia, como ciberacoso, sextorsión y explotación sexual en línea.

SÉPTIMA

La digitalización ha facilitado la comisión de delitos y la violencia de género digital, tanto por la propia estructura del ciberespacio como por la rapidez de los avances tecnológicos. A pesar de los esfuerzos legislativos, los marcos normativos actuales presentan lagunas y deficiencias, que dificultan la protección efectiva de las mujeres y las personas menores de edad contra la ciberdelincuencia y la violencia digital. La rápida evolución de la tecnología supera, con frecuencia, la capacidad de las leyes para mantenerse al día, dejando a las víctimas sin la protección adecuada. De hecho, el derecho va por detrás en cuanto a su regulación, aunque España es un país avanzado en la regulación penal.

OCTAVA

La falta de armonización legislativa internacional complica aún más la lucha contra los delitos digitales, especialmente cuando los perpetradores operan desde diferentes jurisdicciones. Las tecnologías suponen un nuevo medio para la comisión de delitos previamente ya existentes en el ámbito analógico e, igualmente, han dado lugar a nuevos ilícitos como el *sexting ajeno,* el *stalking o* el *grooming*. Concretamente, 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.

NÓVENA

La naturaleza transfronteriza de la ciberdelincuencia requiere una cooperación internacional efectiva. Las conferencias y acuerdos internacionales son cruciales para el intercambio de conocimientos y la implementación de estrategias globales contra la ciberdelincuencia. La cooperación internacional permite la creación de marcos legales y operativos comunes, facilitando la asistencia judicial mutua y promoviendo el intercambio de mejores prácticas para proteger a las víctimas en el entorno digital.

DÉCIMA

En la recopilación de datos oficiales es necesario detallar el origen y el medio del delito, ya que predomina la ausencia de interrelación entre delitos, de tal forma que los casos de ciberviolencia se subsumen en el

delito más grave sin contabilizar su origen tecnológico. A su vez, esta insuficiencia dificulta el tratamiento de la realidad de la ciberdelincuencia, no pudiéndose así cuantificar ni analizar exhaustivamente los ciberdelitos de género, hecho que complica la implementación de medidas vinculadas.

DECIMOPRIMERA

La falta de formación especializada desde la perspectiva de género en el ámbito de la ciberdelincuencia y la insuficiencia de recursos, tanto materiales como 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 efectivamente a estos delitos. Además, la carencia de recursos específicos destinados a la implementación de programas de apoyo y plataformas seguras para las víctimas agrava la situación, dejando a muchas de ellas sin la protección y el apoyo necesarios. Esta brecha formativa y de recursos perpetúa la vulnerabilidad de las mujeres y niñas en el entorno digital y subraya la urgente necesidad de invertir en formación especializada y en la provisión de recursos adecuados para abordar de manera integral la violencia digital.

DECIMOSEGUNDA

Es alarmante el aumento exponencial de las graves y devastadoras consecuencias que la violencia digital produce en las víctimas, al amplificarse extraordinariamente los efectos lesivos sobre los bienes jurídicos afectados, entre otros: honor, intimidad, dignidad, libertad o integridad moral. La situación de conectividad constante, unida con la rapidez y capacidad de difusión, hacen que la lesión se mantenga en el tiempo y que 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. Junto a ello, el incumplimiento con los previos estereotipos o cánones de belleza e imagen que difunden las redes sociales y los medios de comunicación pueden dar lugar a actitudes de rechazo, exclusión social y discriminación y llegar a desembocar en trastornos alimentarios, actitudes homófobas y similares, lo que genera baja autoestima, ansiedad, angustia y aislamiento. La violencia digital amplifica la vulnerabilidad de las mujeres y personas menores de edad, perpetuando las desigualdades de género existentes y creando nuevas formas de victimización en el espacio digital.

DECIMOTERCERA

Las *deepfakes* son sexistas hacia las mujeres, porque las mujeres son relegadas a la esfera privada o al ámbito de lo sexual, cosificándolas. Mientras que los hombres, aunque se les cambie su imagen física o discurso y mayoritariamente aparezcan vestidos, no pierden su esencia de prevalencia en la esfera pública.

DECIMOCUARTA

Dada la complejidad del fenómeno, es urgente abordar los desafíos asociados con la violencia digital, implementando estrategias y políticas efectivas desde una perspectiva de género y de infancia para

proteger a mujeres y las personas menores de edad en el entorno digital y promover una cultura de igualdad y respeto. Una respuesta coordinada es esencial para minimizar los riesgos intrínsecos a las TIC.

PROPUESTAS

La transformación digital es un proceso en constante evolución que implica nuevos retos que hay que afrontar para crear un entorno en línea seguro, predecible y digno de confianza. Por ello, se realiza una serie de propuestas:

1.

Como existen diversas definiciones de «violencia digital», se propone como posible definición universal, 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 expuestos, resulta imprescindible abordar la implementación de medidas para la prevención de la violencia de género en el ámbito digital. 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.

Resulta indispensable una mayor concienciación sobre qué acciones son constitutivas de la violencia digital y de sus consecuencias. Para ello, se recomienda el desarrollo de campañas específicas de sensibilización, concienciación, prevención y detección con perspectiva de género y de infancia y adaptadas al avance de la tecnología en cada momento. Estas campañas deberán reflejar las distintas posiciones de víctimas, agresores o de otras personas involucradas en la agresión y sus distintas consecuencias o mecanismos de protección o denuncia. Esta medida es una manera útil y eficaz de visibilizar el problema, siendo fundamental contar con leyes y políticas que protejan a las víctimas y sancionen a los agresores, así como brindarles apoyo y recursos adecuados para superar las consecuencias de la violencia.

4.

El asesoramiento especializado a las víctimas en todas las fases del procedimiento judicial se presenta como una medida a adoptar de manera inmediata. Esta orientación no debe limitarse al ámbito jurídico, sino que debe abarcar también 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.

La formación especializada y multidisciplinar con enfoque de género de todos los y las profesionales que intervienen en los procesos por casos de violencia digital: fuerzas y cuerpos de seguridad, abogacía, judicatura, equipos psicosociales adscritos a los juzgados, etc. Ello facilitaría la persecución, imputación y sanción de los delitos tecnológicos, a la vez que permitiría una mejor atención a las víctimas y reparación del daño.

6.

Resulta altamente recomendable la creación de protocolos específicos unificados y adaptados a la violencia digital en todos los ámbitos, incluyendo el educativo, sanitario, judicial y policial.

7.

Se recomienda tipificar un delito de usurpación de identidad digital, ya que, en nuestro ordenamiento jurídico, no existe una respuesta penal adecuada, sin perjuicio de la posibilidad de resolver estas situaciones en el ámbito administrativo o, incluso, en el marco de la jurisdicción civil. Al respecto, actualmente nuestro CP limita la sanción de esta conducta a 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.

Es claro que 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 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.

Igualmente, es preciso contar con expertos en informática forense y técnicas de extracción, análisis y preservación de la evidencia digital tanto en las fuerzas y cuerpos de seguridad como en los propios juzgados, dada la naturaleza y características de la prueba digital.

9.

La estadística es una herramienta fundamental para la interpretación de la problemática de la ciberviolencia. Por consiguiente, se propone la elaboración de una estadística propia e interrelacionada

con aquellos delitos que se cometen fuera de la esfera virtual y que tienen su origen en ella. Del mismo modo, estas cifras deben estar disgregadas por sexo, con el fin de determinar su alcance real.

10.

En relación con el acceso de las personas menores de edad a contenidos pornográficos, se manifiesta la necesidad de implicación de las instituciones educativas y de las familias en su educación afectivo sexual, con el fin de contribuir a su desarrollo personal y emocional de manera integral. Es una obligación del Estado implementar acciones específicas orientadas a impedir el acceso de menores a la pornografía en Internet, que dificulta el desarrollo de una sexualidad saludable en la adolescencia y la infancia y, a su vez, promueve prácticas agresivas y denigratorias, además de limitar la capacidad de establecer relaciones basadas en el respeto mutuo, el consentimiento y el placer compartido.

11.

El desarrollo de estrategias y acciones de protección específica de los datos de menores almacenados en Internet.

La implementación de medidas de mejora en la alfabetización mediática, incidiendo en una educación que integre una seguridad en Internet que pueda servir como mecanismo de prevención de lucha contra los peligros del mundo *online*.

Instaurar programas de buenas prácticas de las TIC para progenitores y para menores, estableciendo como «obligatorios o muy recomendables» los mecanismos de control parental en los dispositivos para bloquear contenido violento o sexual inadecuado para su edad.

12.

Como se reclama desde los distintos instrumentos normativos, se debe fomentar la colaboración entre los gobiernos, las autoridades y las organizaciones civiles para identificar nuevas formas de explotación en línea, y desarrollar estrategias que permitan la prevención y la lucha contra la trata de personas, especialmente con fines de explotación sexual, en los entornos digitales.

13.

El desarrollo de la IA conduce a la implementación de políticas y de normativas idóneas que garanticen su uso ético y seguro. En este sentido, habrá que estar en alerta del contenido y cumplimiento de las directrices establecidas en la reciente Ley de IA.

14.

Tipificar como un nuevo delito contra la integridad moral aquellos supuestos en los que alguien 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. Imponer la misma pena de este nuevo delito a quien, habiendo recibido la imagen o grabación manipulada, contribuya a su difusión, revelación o cesión a terceros. Parece que esta cuestión quedará resuelta con el nuevo artículo 173 bis del Anteproyecto de Ley Orgánica para la protección de los menores de edad en los entornos digitales.

15.

Con respecto al uso de las redes sociales y las nuevas tecnologías, la información y la formación facilitadas, deberán enfocarse no como autopuestas en peligro, esto es, no sólo desde la desconfianza y el miedo, sino también orientadas a facilitar mecanismos de protección, control, identificación y detección de riesgos, esto es, para generar autoprotección.

16.

Se recomienda instaurar formación transversal y obligatoria continua, adecuada y especializada con perspectiva de género digital, con contenidos actualizados tanto para familias, menores y adolescentes como para profesionales de los distintos ámbitos.

ANEXO

TALLER CON PROFESIONALES ESPECIALISTAS EN LA MATERIA.

Para completar el estudio, se llevó a cabo un taller con profesionales especialistas de los diferentes ámbitos de intervención con víctimas de violencia en el campo digital.

Como paso previo a la celebración del taller, y para organizar mejor las materias a abordar, poder debatir sobre las mismas y obtener conclusiones, se elaboró un breve cuestionario y se remitió a los y las distintas profesionales de todos los ámbitos (Agencia de Protección de Datos, Fiscalía en materia de Cibercriminalidad Informática, universidad y fuerzas y cuerpos de seguridad) para que la constestaran.

Se convocó a los especialistas al encuentro de trabajo, que se celebró en la sede de la Asociación, conjuntamente con las autoras de la investigación. La finalidad era poner en común conocimientos y experiencias para analizar en qué medida se cumplen las obligaciones de protección, persecución, castigo a los autores y reparación a las víctimas de estos delitos, realizar propuestas para mejorar y obtener conclusiones, así como tratar de profundizar en la construcción y reflexión grupal para, mediante las aportaciones y experiencias de los y las participantes, detectar dificultades, realizar propuestas de buenas prácticas y mejora, y obtener conclusiones comunes.

Tras la lectura de los formularios recibidos y el cierre del taller, se extraen una serie de conclusiones para detectar los errores que se están cometiendo y plantear propuestas para su corrección, así como marcar unas pautas de buenas prácticas y mejoras, que permitan una atención coordinada y especializada en cada ámbito profesional y conjuntamente en la materia.

Siguiendo las reseñas marcadas en el cuestionario, son destacables las siguientes cuestiones que exceden de la práctica procesal:

- Con carácter general, se observa un progreso gradual en la comprensión de las ventajas, inconvenientes y riesgos de las acciones realizadas en línea. Sin embargo, se ha identificado una tendencia mayoritaria en la información disponible que suele enfocarse en la desconfianza y el miedo hacia las nuevas tecnologías, en lugar de proporcionar herramientas para protegerse y detectar riesgos.

  Por lo tanto, es esencial ampliar la información existente para incluir mecanismos de autoprotección y concienciación sobre las posibles consecuencias de la realización de ciertos comportamientos.

  Es crucial crear un entorno seguro y abierto en Internet. La información se debe enfocar en campañas de prevención y sensibilización, ya que la generalización de las tecnologías de la información y la comunicación, debido a su alto nivel de conectividad y su potencialidad para la elaboración y difusión de todo tipo de contenidos, ha facilitado conductas perjudiciales, como el acoso sexual a menores y la producción, distribución y puesta a disposición de terceros de material pornográfico ilegal.

En cuanto a la implementación de planes formativos se destaca positivamente la labor del Instituto Nacional de Ciberseguridad.[210]

- La recogida de datos es fundamental para conocer el alcance y evolución de la violencia digital. En relación con las estadísticas publicadas por el Ministerio del Interior y por la Fiscalía General del Estado, sería recomendable poder establecer la interrelación entre los distintos tipos penales que pudieran concurrir con los supuestos delictivos cometidos mediante el empleo de las tecnologías de la información y de la comunicación y su desagregación por sexo. Según la Fiscalía, en algunos casos no especificados, el contacto con menores a través de tecnologías de la información y la comunicación (TIC) con fines sexuales no se refleja estadísticamente cuando se logra el objetivo deseado, ya que se considera parte de la infracción más severamente castigada.

- Normalmente, las campañas de sensibilización, concienciación, prevención y detección son una manera útil y eficaz de visibilizar el problema. Los y las profesionales consideran que son fundamentales y positivas, pero no suficientes, por lo que han de adaptarse a la casuística y evolución de la tecnología en cada momento. Además, deben plantearse desde distintos enfoques, desde la perspectiva de la víctima, del agresor o de otras terceras personas que intervienen en la agresión, y de las consecuencias desde cada posición.

  Se proponen otras formas de concienciación como pueden ser: visionado de vídeos explicativos en redes sociales, series de televisión o concursos en centros educativos, infografías o trabajos de investigación.

  Se tendrá que determinar cuáles son las causas de la violencia en Internet y en cualquiera de sus manifestaciones, y se debería impartir una formación básica en materia emocional y empatía.

- Es fundamental promover la colaboración y el intercambio de información entre los diferentes actores involucrados en la lucha contra la ciberdelincuencia. No sólo los operadores encargados de la investigación y persecución penal, sino también aquellos que tienen la responsabilidad de fomentar un uso seguro de las tecnologías. Es necesario trabajar de forma abierta y en conjunto con organismos como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Nacional de Protección de Infraestructuras Críticas y Ciberseguridad (CNPIC) y la Oficina de Coordinación de Ciberseguridad (OCC) para compartir experiencias, conocimientos y buenas prácticas en este ámbito. Es necesario que esta actuación colaborativa alcance también al sector privado, fundamentalmente a operadores de comunicaciones y proveedores de servicios en Internet y a los grupos de investigación universitaria.

- Los y las profesionales reconocen que las medidas de control y prevención disponibles en las distintas plataformas son insuficientes, ya que, aunque las principales redes sociales permiten la denuncia al proveedor de servicios y toman medidas, no siempre lo hacen con la rapidez

[210] Instituto Nacional de Ciberseguridad (INCIBE) es una institución dependiente del Ministerio para la Transformación Digital y de la Función Pública para el desarrollo de la ciberseguridad y de la confianza digital de la ciudadanía, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

necesaria debido a la complejidad del ciberespacio. Además, se enfrentan a dificultades debido a las diferentes jurisdicciones de los países en los que operan las plataformas y redes sociales, lo que requiere de cooperación internacional para su adecuada regulación.

En cuanto a las medidas de control y prevención, se destaca positivamente el canal de denuncia de la Agencia Española de Protección de Datos, así como la confianza en la implementación del Reglamento UE 2022/2065, que modifica la Directiva 2000/31/CE en la Unión Europea, estableciendo obligaciones para el control de contenidos en redes sociales, responsabilidades para las plataformas en línea y regulaciones para combatir contenidos ilícitos, discursos de odio y desinformación.

- Se plantea el estudio de la utilización de la inteligencia artificial para filtrar contenido violento en redes sociales, rebajando al mínimo la intervención humana para evitar los posibles daños y secuelas que se han advertido entre los y las moderadores/administradores de contenido.
- Por lo general, se detecta una falta de formación especializada entre los y las profesionales intervinientes, desconocimiento en el tratamiento y conservación de la prueba y falta de conocimiento técnico por los operadores jurídicos y profesionales que intervienen en el proceso.

  Por ello, la formación transversal debería ser requisito imprescindible. Implementar formaciones continuadas, adecuadas y especializadas, con contenidos actualizados para familias, menores y adolescentes y profesionales de distintos ámbitos intervinientes: educativo, sanitario, fuerzas y cuerpos de seguridad, asistencial, operadores jurídicos (abogadas/os, peritos judiciales, jueces/zas, fiscales/as, etcétera). Deberá hacerse hincapié en las consecuencias nocivas que se derivan, con mayor intensidad en algunos casos que en el mundo analógico, de las actuaciones en red para determinados bienes jurídicos.

  En el caso de las fuerzas y cuerpos de seguridad, la formación es escasa y no alcanza a los puestos operativos, faltan recursos y se aboca a la autoformación. En la recolección de la prueba digital, la formación desatiende las necesidades concretas y especialidades de volatilidad, inmediatez y urgencia, basando, en muchos casos, la recopilación de la prueba a la experiencia individual de cada profesional y predeterminada.
- La Agencia de Protección de Datos, junto con el Gobierno de España y expertos/as en la materia, se encuentra trabajando en la futura *Ley de protección a la infancia y la juventud en el ámbito digital*. Por su parte, *el Consejo de Ministros ya ha aprobado el Anteproyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales*. Entre otras cuestiones a tratar, en esta nueva norma se plantea el establecimiento de una formación a familias, incluyéndose la prevención en cuanto a los perjuicios en la salud pública y mental del consumo inadecuado de Internet y del empleo de violencia a través de la red dentro de los primeros protocolos del niño/a sano.
- Se detecta la necesidad de enseñar en los colegios la posible responsabilidad penal, es decir, que los menores y adolescentes sepan que cuando realizan determinadas conductas están cometiendo un delito.

- En general, se destaca la inexistencia de protocolos unitarios para los y las distintas profesionales de los distintos ámbitos o desconocimiento de su existencia. Se hace necesaria su instauración, además de ser fundamental la creación de protocolos relacionados con el mantenimiento y conservación de prueba en aras a evitar la perpetuación de la situación de victimización.

  Valorar positivamente el protocolo firmado el 21 de diciembre del 2022, entre Fiscalía General del Estado, a través de la Unidad de Criminalidad Informática y el Instituto de Ciberseguridad de España (INCIBE), a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, por el que colaborarán en el marco del servicio de línea directa o *hotline* que gestiona INCIBE, para potenciar y reforzar las actuaciones que tienen por objeto la investigación y persecución de los actos de agresión sexual *online* a menores y los relacionados con el material de abuso sexual infantil.

- Es reseñable considerar que las tecnologías no necesariamente implican favorecer la comisión del delito, ya que algunos tipos se venían produciendo en el ámbito analógico, sino que suponen un nuevo medio para su realización. Aumentan exponencialmente las graves consecuencias que producen en las víctimas, al amplificarse extraordinariamente los efectos lesivos sobre los bienes jurídicos afectados, entre otros: honor, intimidad, dignidad, libertad, integridad moral. La situación de conectividad constante, unida con la rapidez y capacidad de difusión, hacen que la lesión se mantenga en el tiempo y que alcance a un gran número de personas.

  A esto hay que añadir que las tecnologías facilitan el control de las víctimas de violencia machista y el grado de accesibilidad a las mismas. También, hay que mencionar la aparición de nuevos tipos delictivos como el *grooming*, *sexting*, etc., que han tenido que ser objeto de regulación legislativa.

- Merece la pena destacar que, con relación a la trata de mujeres con fines de explotación sexual, el ámbito digital ha favorecido la captación, ofrecimiento y control de las víctimas.

  En este sentido, la Fiscal de Sala Coordinadora de la Unidad de Trata de Personas y Extranjería alegó en el Día Mundial contra la Trata de Seres Humanos en el año 2022: «*tras la pandemia se acrecentó el uso de las nuevas tecnologías y las redes sociales, para captación, ofrecimiento y el control de las víctimas. Por otro lado, se ha aumentado el consumo de pornografía, y algunas ONGs alertan de que parte de la explotación sexual se ha trasladado a entornos virtuales, aunque lo cierto es que aún no hemos detectado casos de trata en este ámbito, pero es algo que habrá que explorar, especialmente a través del rastreo de redes. En mi opinión, la pornografía no ha sustituido a la prostitución física, simplemente ambas conviven*».

- En líneas generales, se puede afirmar que hay una serie de factores característicos de la comisión de delitos mediante el empleo de las TIC que influyen en la sensación de impunidad de esta tipología delictiva. Son destacables los siguientes:

  - El anonimato, que permite la ocultación de la identidad, dificulta la persecución, la identificación y la imputación.

  - La falta de fronteras de la red, que facilita que los delincuentes operen desde diferentes países haciendo depender de la cooperación internacional la persecución y sanción del delito, con la dificultad que implica.

- El dinamismo de Internet, que conlleva la necesidad de actualización constante para conocer las últimas tecnologías y recibir la formación adecuada y especializada en la materia.
- La propia evolución y dinamismo de la red.

Aunque las denuncias poco a poco están creciendo, debido a que cada vez hay un mayor conocimiento sobre los actos que pueden ser considerados delictivos, en la actualidad sigue habiendo factores que condicionan la interposición de denuncia, como pueden ser: el temor al estigma, no saber que están siendo víctimas de un delito o percibir que el proceso judicial no será efectivo.

- Es necesario crear una unidad especializada en la investigación, detección y prevención dentro de cada uno de los cuerpos y fuerzas de seguridad con criterios unificados de recolección y conservación de prueba. El resto de agentes que no pertenezcan a estas unidades técnicas deberán recibir una formación mínima en la materia.
- Se detecta una necesidad extendida de recursos materiales y humanos.
- La cooperación internacional es compleja y está circunscrita a los convenios firmados en el seno del Consejo de Europa. Se observa que las sinergias y preocupación generadas entre Estados en torno a la protección frente a la ciberdelincuencia cuando los bienes afectados son de carácter económico, por ejemplo, defraudaciones o delitos contra la propiedad intelectual, no se produce de la misma manera en las lesiones a derechos de carácter personalísimo. Es destacable que, en el marco de la Unión Europea, existe menor dificultad en la persecución y sanción del delito que con aquellos países en los que no existe convenio de cooperación o que se encuentran fuera de su ámbito de aplicación, en cuyo caso, la colaboración se vuelve más compleja.
- Resulta imprescindible detectar los riesgos del uso inadecuado del medio tecnológico, educar en prevención y formar a los educadores y familias e impartir formación en valores éticos esenciales.

  En este sentido, la Ley 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia establece que las administraciones públicas competentes regularán planes y programas de prevención para la erradicación de la violencia sobre la infancia y la adolescencia, identificando grupos de riesgo, y medidas de detección precoz frente a procesos de aprendizaje de modelos de conductas violentas o de conductas delictivas. Así, acoge una serie de capítulos dedicados a la prevención de la violencia contra los y las menores desde diferentes ámbitos.

  En el ámbito familiar establece que las Administraciones deberán prestar a las familias apoyo para prevenir desde la primera infancia factores de riesgo, así como el impulso de medidas de política familiar en torno a una parentalidad positiva.

  En los centros educativos habría que instaurar un plan de convivencia con protocolos frente al acoso escolar, sexual o ciberacoso entre otros. Además, resulta necesaria la constitución de la figura del coordinador o coordinadora de bienestar y protección, que deberán tener todos los centros educativos públicos, concertados o privados de educación infantil, primaria y secundaria, conforme establece el artículo 35 de la Ley 8/2021, de 4 de junio, de protección

integral a la infancia y la adolescencia frente a la violencia, además de garantizar el aprendizaje de un uso seguro y respetuoso de los medios digitales.

En la esfera sanitaria, se recomienda la elaboración de protocolos de actuación para la promoción del buen trato, la identificación de factores de riesgo y la prevención y detección precoz de la violencia en menores y adolescentes.

- En relación con la solicitud del DNI o cualquier otro tipo de identificación que no garantice el anonimato al acceder al ciberespacio, como medida para facilitar la imputación de los delitos tecnológicos, se considera un mecanismo disuasorio, pero de difícil implementación, como consecuencia del propio derecho al anonimato defendido en el entorno virtual. De la misma forma, esta solicitud de identificación podría chocar con, por ejemplo, la figura del agente encubierto que, precisamente, utiliza ese anonimato para la investigación criminal a través de la infiltración en un grupo en RRSS o su intervención o localización de pruebas. Por ello, son aconsejables medidas que permitan el pseudoanonimato, recogido en la carta de derechos y deberes digitales.
- Es interesante el sistema de verificación de edad propuesto por la Agencia de Protección de Datos para la protección de menores en Internet. Se ha basado en los modelos europeos, con un sistema de doble ciego, de tal modo que, cuando se accede a una página mediante este sistema de verificación, no se dispondrá de datos de identificación, ni de edad, ni de contenido. También es destacable la advertencia en diferentes páginas web mediante un etiquetado que refiera «contenido para adultos».
- Mencionar que la legislación penal se ha ido adaptando, reformando y creando nuevas tipologías delictivas para evitar la impunidad de conductas realizadas a través de medios tecnológicos y de la comunicación. El uso generalizado de las TIC ha supuesto un nuevo medio para cometer delitos que, en muchos casos, ya estaban previstos en nuestro Código Penal.

CUESTIONARIO PARA PROFESIONALES

Dentro de las actividades programadas en el “Estudio y respuesta judicial sobre ciberviolencia y su impacto en las mujeres y menores”, que está realizando la Asociación de Mujeres Juristas Themis, se encuentra la realización de un taller con profesionales de los diferentes ámbitos de intervención con víctimas de delitos cometidos a través de las TIC.

La finalidad de este taller es poner en común conocimientos y experiencias para analizar en qué medida se cumplen las obligaciones de protección, persecución, castigo a los autores y reparación a las víctimas de estos delitos, así como realizar propuestas para mejorar y obtener conclusiones.

Como paso previo a la celebración del taller, y para organizar mejor las materias a abordar y debatir y las intervenciones que se realicen, le rogamos que cumplimente este cuestionario.

Le agradecemos de antemano su contribución que, a buen seguro, servirá para mejorar la atención que desde los diferentes ámbitos se da a las víctimas de la violencia en el ámbito digital.

Normas para cumplimentar el cuestionario:

- Conteste a las preguntas de manera breve.
- Al final hay un campo de observaciones donde puede añadir lo que considere oportuno.

1. **En su opinión, ¿en la actualidad se cuenta con información suficiente acerca de los riesgos que sufren los y las menores en el ámbito digital?**
2. **¿Cree que existen suficientes datos sobre la respuesta penal a la violencia contra las mujeres y l@s menores cometida en el ámbito digital? ¿Cree necesario que se lleve a cabo de manera sistemática y periódica la recogida de datos y que se realicen estadísticas e investigaciones sobre violencia hacia las mujeres y l@s menores en el ámbito digital y su relación con los delitos tradicionales?**
3. **¿Cree que las campañas de sensibilización para la prevención y detección de la violencia de género digital en menores y adolescentes, su entorno familiar y docente que se han realizado son suficientes? ¿Aparte de las campañas publicitarias, se le ocurren otras formas de concienciación de la violencia?**
4. **En su opinión, ¿considera que desde las distintas plataformas (redes sociales y servicios de mensajería instantánea) se disponen de suficientes medidas de control y prevención de la violencia digital?**
5. **En cuanto a la prevención como profesionales y, dada su experiencia, ¿qué medidas implementaría?**
6. **¿Considera necesaria la elaboración de protocolos y planes de actuación y coordinación que sean específicos para la violencia cometida a través de las nuevas tecnologías? ¿Conoce si existe alguno en su ámbito profesional de intervención?**
7. **¿Cree que existe una coordinación adecuada entre los diferentes ámbitos de actuación? ¿Puede concretar, desde su ámbito profesional, con qué instituciones existe esa coordinación y con cuáles otros sería necesario establecerla?**
8. **¿Considera que el grado de formación especializada en violencia digital en los diferentes ámbitos profesionales que intervienen es adecuado?**
   ¿En qué ámbitos considera que debería de implementarse la formación especializada? Fuerzas y cuerpos de seguridad/sanitario/servicios sociales/judicial/educativo.
   ¿Cree que dicha formación especializada debería impartirse tanto a profesionales de servicios generales como a profesionales de servicios especializados?
9. **¿Cuáles de los siguientes ámbitos considera deben estar comprendidos en el marco de los servicios generales?**
   Asesoramiento jurídico
   Atención psicológica
   Educación
   Peritaje informático

10. **¿Le parece adecuado que dentro de los servicios especializados se contemplen?**

11. **En su opinión, ¿cree que las nuevas tecnologías han facilitado la comisión de delitos de violencia de género?**

12. **¿Qué problemas se ha encontrado en su profesión en relación con la trata de mujeres con fines de explotación sexual desde el punto de vista digital?**

13. **Parece una percepción extendida la impunidad que existe en relación con la violencia de género cometida utilizando las nuevas tecnologías ¿comparte dicha percepción?**

    ¿Cuál cree que es la causa? (Legislación existente, su aplicación por juzgados y tribunales, la falta de recursos humanos y/o materiales, formación de profesionales, formación en concienciación de riesgos).

    ¿Cree que deberían abordarse las reformas legales necesarias para restaurar la confianza de las víctimas en el sistema penal? ¿o cree que es más necesaria la concienciación previa de adolescentes y familiares?

    ¿Cuáles de las siguientes considera necesarias?

    – Creación de juzgados especializados para su enjuiciamiento.
    – Solicitud de DNI para alta en redes sociales.
    – Regulación de medidas de protección con carácter obligatorio (medios audiovisuales para tomar declaración preconstituida, equipos forenses especializados (medicina general, psicología, psiquiatría).
    – Mejorar medidas cautelares de protección (retirada de contenidos, cierre de negocios, etcétera).
    – Normas sustantivas penales.

14. **¿Cree necesario revisar y, en su caso, modificar la legislación penal?**

15. **¿Considera que existe una cooperación internacional adecuada y efectiva? ¿Cómo cree que se podría mejorar?**

    ¿Qué aspectos cree que es imprescindible abordar en relación con la violencia digital hacia los y las menores y las mujeres? Por favor, indíquelos en orden de prioridad.

BIBLIOGRAFÍA

Referencias bibliográficas

ALCÁNTARA, J.; «La neutralidad de la Red y porqué es una mala idea acabar con ella», *Biblioteca de las Indias*, Madrid, 2011, pp. 10 y ss.

ARÁNGUEZ SÁNCHEZ, T.; «Tres modelos legislativos de la pornografía», *Revista Internacional de Estudios Feministas*, v 6, n.º 1, 2021, pp. 165-189.

ARÁNGUEZ SÁNCHEZ, T., OLARIU O.; Feminismo digital. Violencia contra las mujeres y brecha sexista en internet, 2021.

ANDREU MARTÍNEZ, B.; «Los menores y sus derechos en la sociedad digital», *Sociedad Digital y Derecho,*2018, pp. 417-438.

BALLESTER BRAGE, L., ORTE SOCÍAS, C., y POZO GORDALIZA, R.; «Estudio de la nueva pornografía y relación sexual en jóvenes», *Revista andaluza de Ciencias Sociales*, 2014, n.º 13, pp. 165-178.

BONINO MÉNDEZ, L.; «Los micromachismos», *Revista La Cibeles,* n.º 2, 4.

CANO TERUEL, Q.; «Ciberdelencuencia en el Código Penal», *cibercrim*, 2024.

DELGADO MARTÍN, J.; «La prueba digital. Concepto, clases, aportación al proceso y valoración», *Diario La Ley,* Sección Ciberacoso, 2017, n.º 6.

DELGADO MARTÍN, J.; «Investigación tecnológica y prueba digital en todas las jurisdicciones», 2ª edición actualizada, Madrid, *La Ley Wolters Klumer*, 2018.

DELGADO MARTÍN, J.; «Prueba Digital Internacional. El Reglamento E-Evidence», *Diario La Ley*, 2023, n.º 76.

DEVÍS MATAMOROS, A.; «Algunas claves del castigo penal del deepfake de naturaleza sexual», ibericonnect.blog, 2023

DÍEZ PERALTA, E.; «Los derechos de la mujer en el Derecho internacional», *Revista española de derecho internacional*, 2011, v. 63, n.º 2, pp. 87-121.

DÍAZ PERALTA, E.; «El matrimonio infantil y forzado en el Derecho internacional: Un enfoque de género y de derechos humanos», Valencia, *Tirant lo Blanch*, 2019, pp. 10-15.

GARCÍA COLLANTES, A., GARRIDO ANTÓN M. J.; «Violencia y ciberviolencia de género», Valencia, *Tirant lo Blanch*, 2021.

GING, D., SIAPERA, E.; «*Special issue on online misogyny», en* Feminist Media Studie*, Routledge Taylor & Francis Group*, 2018, v. 18, n.º 4, pp. 515-524.

GÓMEZ MIGUEL A., SANMARTÍN ORTÍ A., y KURIC KARDELIS S.; «Videojuegos y jóvenes: lugares, experiencias y tensiones», DOI: 10.5281/zenodo.7970990, 2023.

LLORIA GARCÍA, P. (directora), CRUZ ANGELES, J. (coordinador); «La violencia sobre la mujer en el S.XXI: género, derecho y TIC», Pamplona, *Aranzadi Thomson Reuters*, 2019.

LLORIA GARCÍA, P.; «La regulación penal en materia de violencia familiar y de género tras la Reforma de 2015. Especial referencia al ámbito tecnológico». *Revista General de Derecho Penal,* 2019, n.º 31, pp. 30-32.

LLORIA GARCÍA, P.; «Violencia sobre la mujer en el s. XXI. Violencia de control y nuevas tecnologías. Habitualidad, sexting y stalking», Madrid, Iustel, 2020.

LLORIA GARCÍA, P.; «La difusión de imágenes íntimas sin consentimiento (A propósito de la Sentencia 70/2020 del Tribunal Supremo de 24 de febrero de 2020)», en *La Ley Privacidad*, 2020, n.º 4, pp.1-9.

LLORIA GARCÍA, P.: «Algunas reflexiones sobre el concepto de delito tecnológico y sus características», en LEÓN ALAPONT, J., GONZÁLEZ CUSSAC, J.L.; «Estudios jurídicos en memoria de la Profesora Doctora Elena Górriz Royo», Valencia, *Tirant lo Blanch*, 2020.

LLORIA GARCÍA, P.; «La LO 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia y la transformación del Código Penal. Algunas consideraciones», *Igualdad. ES*, 2022, n.º 6, pp. 271-298.

LLORIA GARCÍA, P.; «El delito de *Child grooming* y el consentimiento de menores de 16 años (arts. 183 y 183 bis del CP)», en MARTÍNEZ GALINDO, G., MAESTRE DELGADO, E.; «La reforma de los delitos sexuales», *J.M Bosch*, Madrid, 2024.

MANJÓN-CABEZA OLMEDA, A.; «La mujer víctima de la violencia de género. (Legislación penal y Sentencia del Tribunal Constitucional 59/2008, de 14 de mayo)», en MARTÍNEZ FRANCISCO, M.N., GARCÍA-PABLOS DE MOLINA, A., MIRANDA DE AVENA, C.; «Víctima, prevención del delito y tratamiento del delincuente». Granada, *Comares*, 2009, pp. 43-74.

MAQUEDA ABREU, M. L.; «La violencia de género: Entre el concepto jurídico y la realidad social». *Revista Electrónica de Ciencia Penal y Criminología*, 2006, n.º 8.

MARTÍNEZ DE PISÓN CAVERO, J. M.; «La identidad de género en el Tribunal Europeo de Derechos Humanos». *Anuario de filosofía del derecho*, 2022, n.º 38, pp. 105-136.

MARTÍNEZ ESCAMILLA, M.; «La ligereza del Tribunal Supremo ante las víctimas de trata. Sentencia 960/2023 de la Sala Segunda del Tribunal Supremo, de 21 de diciembre», *Crítica Penal y Poder*, (Dossier «Migración y trata. Algunas sentencias relevantes»), 2024, n.º 26.

MARTÍNEZ GALINDO, G.; «La reforma de los delitos sexuales», *J.M Bosch*, Madrid, 2024, pp. 201-234.

MIRÓ LLINARES, F.; «El cibercrimen: fenomenología y criminología de la delincuencia en el ciberespacio», Madrid, *Marcial Pons*, 2012.

MIRÓ LLINARES, F.; «Cometer delitos en 140 caracteres: El derecho penal ante el odio y la radicalización en Internet». Madrid, *Marcial Pons*, 2017, pp. 10-12.

MORALES PRATS, F.; «Los ilícitos en la red (II): pornografía infantil y ciberterrorismo», en ROMEO CASABONA, C.M.; «El cibercrimen», Granada, *Comares*, 2006, pp. 271-297.

MORALES PRATS, F.; «Pornografía infantil e Internet: la respuesta en el Código Penal español», en MARTÍN-CASALLO LÓPEZ, J.J., «Problemática jurídica en torno al fenómeno de Internet», *Cuadernos de derecho judicial*, 2000, n.º 4, pp. 175-205.

MORENO ACEVEDO, R.; «Los delitos relativos a la captación o utilización con fines exhibicionistas o pornográficos, o para la elaboración de pornografía infantil, art. 189.1 a)». *Revista Electrónica de Ciencia Penal y Criminología*, 2023.

MUÑOZ CONDE, F.; «Derecho Penal. Parte Especial», Valencia, *Tirant lo Blanch*, 2023.

PÉREZ MARTÍNEZ P., FRÍAS BARROSO, Z., UREÑA LÓPEZ, A.; «50 años de la red de redes. La evolución de Internet en España: del Tesys a la economía digital», Red.es, 2018.

QUEVEDO GONZÁLEZ, J.; «Investigación y prueba del ciberdelito», Madrid, *Sepin*, 2017.

QUERALT JIMÉNEZ, A.; «Desinformación por razón de sexo y redes sociales», *International Journal of Constitutional Law*, v. 21, n.º 5, 2023, pp. 1589–1619.

SÁNCHEZ BENÍTEZ, C.; «Tratamiento jurídico-penal del acoso en España. Especial referencia a las Leyes Orgánicas 4/2022, de 12 de abril y 10/2022, de 6 de septiembre», BOE. Derecho Penal y Procesal Penal, 2023.

TAMARIT SUMALLA, J. M.; «Cibersexo transaccional: victimización en la intervención penal» *IDP: revista de Internet, derecho y política*, 2022, n.º 37, pp.2-4.

TAMARIT SUMALLA, J.; «La victimología como fundamento del estatuto de las víctimas de delitos», *Revista Internacional de Victimología e Justicia Restaurativa*, 2023, v. 1, n.º 1, pp. 127-140.

VALLE MARISCAL DE GANTE, M.; «La sentencia de 2 de noviembre de 2021 del Tribunal Superior de Justicia de Cataluña: un importante paso hacia adelante en la protección de las víctimas de trata», Diario La Ley, 2022, n.º 9986.

VILLACAMPA ESTIARTE, C.; «La trata de seres humanos tras la reforma del Código Penal de 2015», *Diario La Ley*, 2015, n.º 8554.

VILLEGA-SIMÓN, I; NAVARRO, C.; «Influencers digitales y el feminismo: del activismo al *self-branding*», *en* Los Derechos de la Mujeres en la era de Internet, Universidad de Granada, 2021.

YELA UCEDA, M.; «Estatuto de refugiada por motivos de género, blindaje de fronteras y desafíos actuales en la UE». *FEMERIS: Revista Multidisciplinar de Estudios de Género*, 2022, v. 7, n.º 2, pp.142-157.

YELA UCEDA, M.; «La protección de los derechos de los refugiados desde el punto de vista del derecho Internacional penal», Pamplona, *Aranzadi*, 2023.

YELA UCEDA, M.; «Análisis multidisciplinar sobre las posibles vulneraciones de derechos en el uso de la inteligencia artificial en el Derecho Penal», en ROPERO CARRASCO, J. (Coord.) «Aspectos jurídicos de actualidad en el ámbito del Derecho Digital», *Tirant Lo Blanch*, 2023, pp. 380-382.

YELA UCEDA, M.; «Oportunidades y potenciales riesgos de la aplicación de la inteligencia artificial en herramientas para la prevención de delitos», en JIMÉNEZ GARCÍA, F., Y SÁNCHEZ GARCÍA, B.;

«La atribución de una responsabilidad jurídico penal e internacional de la Inteligencia Artificial», *Iustel*, 2023.

Referencias normativas

Nacionales y autonómicas

Ley Orgánica 1/2004, de 28 de diciembre, de Medidas de Protección Integral contra la Violencia de Género. Boletín Oficial del Estado núm. 313, 29 de diciembre de 2004.

Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre. Boletín Oficial del Estado núm. 152, de 23 de junio de 2010.

Ley Orgánica 1/2015, de 30 de marzo, por la que modifica la Ley Orgánica 10/1995, de 23 de noviembre. Boletín Oficial del Estado núm. 77, de 31 de marzo de 2015.

Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación. Boletín Oficial del Estado núm. 340, de 30 de diciembre de 2020.

Ley Orgánica 8/2021, de 4 de junio, de protección integral a la infancia y la adolescencia frente a la violencia. Boletín Oficial del Estado núm. 134, de 05 de junio de 2021.

Ley Orgánica 3/2022, de 31 de marzo, de ordenación e integración de la Formación Profesional. Boletín Oficial del Estado núm. 78, de 01 de abril de 2022.

Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual. Boletín Oficial del Estado núm. 215, de 07 de septiembre de 2022.

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. Boletín Oficial del Estado, núm. 51, de 01 de marzo de 2023.

Andalucía

Ley 7/2018, de 30 de julio, por la que se modifica la Ley 13/2007, de 26 de noviembre, de medidas de prevención y protección integral contra la violencia de género. Boletín Oficial del Estado núm. 207, de 27 de agosto de 2018.

Castilla-La Mancha

Ley 4/2018, de 8 de octubre, para una Sociedad Libre de Violencia de Género en Castilla-La Mancha. Boletín Oficial del Estado núm. 301, de 14 de diciembre de 2018.

Cataluña

Ley 17/2020, de 22 de diciembre, de modificación de la Ley 5/2008, del derecho de las mujeres a erradicar la violencia machista. Boletín Oficial del Estado, núm. 11, de 13 de enero de 2021.

Galicia

Ley 15/2021, de 3 de diciembre, por la que se modifica la Ley 11/2007, de 27 de julio. Boletín Oficial del Estado, núm. 54, de 4 de marzo de 2022.

La Rioja

Ley 11/2022, de 20 de septiembre, contra la Violencia de Género de La Rioja. Boletín Oficial del Estado, núm. 238, de 4 de octubre de 2022.

Internacionales

Instrumento de Ratificación de 16 de diciembre de 1983 de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer, hecha en Nueva York el 18 de diciembre de 1979. Boletín Oficial del Estado núm. 69, de 21 de marzo de 1984.

Convenio sobre la ciberdelincuencia del Consejo de Europa. Budapest, de 23 de noviembre de 2001.

Directiva 2011/93/UE del Parlamento Europeo y del Consejo de 13 de diciembre, relativa a la lucha contra los abusos sexuales y la explotación sexual de menores y la pornografía infantil y por la que se sustituye la Decisión 2004/68/JAI del Consejo. Diario Oficial de la Unión Europea núm. 335, de 13 de diciembre de 2011.

Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. Diario Oficial de la Unión Europea núm. 218, de 14 de agosto de 2013.

Convenio para la protección de los niños contra la explotación y el abuso sexual del Consejo de Europa. Lanzarote, de 25 de octubre de 2017.

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 (Reglamento de Servicios Digitales). Diario Oficial de la Unión Europea núm. 277, de 27 de octubre de 2022.

Ley 27.736, Ley Olimpia (modificaciones a la ley 26.485) violencia digital. Boletín Nacional de la Nación Argentina, de 23 de octubre de 2023.

Reglamento (UE) 2023/1543 del Parlamento Europeo y del Consejo, de 12 de julio de 2023, sobre las órdenes europeas de producción y las órdenes europeas de conservación a efectos de prueba electrónica en procesos penales y de ejecución de penas privativas de libertad a raíz de procesos penales. Diario Oficial de la Unión Europea núm. 191, de 28 de julio de 2023.

Directiva (UE) 2024/1385 del Parlamento Europeo y del Consejo, sobre la lucha contra la violencia contra las mujeres y la violencia doméstica, Diario Oficial de la Unión Europea núm. 1385, de 24 de mayo de 2024.

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican

los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial). Diario Oficial de la Unión Europea núm. 1689, de 12 de julio de 2024.

Referencias documentales

Agencia Española de Protección de Datos (AEPD). *Marco de Actuación de Responsabilidad Social. AGENDA 2030*. (2019-2024). AEPD, marzo de 2019.

Agencia Española de Protección de Datos (AEPD). *Plan Anual 2024 de Responsabilidad Social*. AGPD, 20 de febrero de 2023.

Agencia Española de Protección de Datos (AEPD). *Protección de datos y prevención de delitos*, AEPD, 16 de mayo de 2018.

Agencia Europea de los Derechos Fundamentales. *Violencia de Género contra las mujeres: una encuesta a escala de la UE*. Agencia de los Derechos Fundamentales de la Unión Europea, Luxemburgo, 2014.

Amnistía Internacional. *#toxictwitter. violencia y abuso contra las mujeres en internet*. Amnistía Internacional, 2018.

Bifdefender. *2024 Consumer Cybersecurity Assessment Report*. Bifdefender, abril de 2024.

Comisión Europea. *Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una Unión de la igualdad: Estrategia para la Igualdad de Género 2020-2025*. Bruselas, 5 de marzo de 2020.

Comisión Europea. *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de la UE sobre los derechos de las víctimas (2020-2025)*. Bruselas, 24 de junio de 2020.

Comisión Europea. *Comunicación de la Comisión al Parlamento europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Una década digital para los niños y los jóvenes: la nueva estrategia europea para un internet mejor para los niños (BIK+)*. Bruselas, 11 de mayo de 2022.

Comisión Europea. *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza*. Bruselas, 19 de febrero de 2020.

Comisión Europea. Propuesta de Reglamento de Inteligencia Artificial. Resolución legislativa del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión.

Comisión Europea. *Propuesta de Directiva (UE) 2024/2486 del Parlamento Europeo y del Consejo, de 5 de marzo de 2024, por la que se establece un paquete normativo para prevenir y combatir el*

abuso sexual de los menores en el entorno digital. Diario Oficial de la Unión Europea, de 5 de marzo de 2024.

Comité Consultivo de Igualdad de Oportunidades entre hombres y mujeres de la Unión Europea. «*New notification: cyberviolence against women has been flagged» Opinion on combatting online violence against women*. 1 de abril de 2020.

Comité Económico y Social Europeo. *Dictamen del Comité Económico y Social Europeo sobre «La publicidad a través de influencers y su impacto en los consumidores»*. 13 de julio de 2023.

Comité Económico y Social Europeo. *Dictamen del Comité Económico y Social Europeo sobre la propuesta de Directiva del Parlamento Europeo y del Consejo sobre la lucha contra la violencia contra las mujeres y la violencia doméstica*. 13 de julio de 2022.

Consejo de Europa y Asociación Internacional de Mujeres Juezas (IAWJ). *Conferencia regional sobre ciberviolencia y pruebas electrónicas. América Latina y el Caribe. Proyectos OCTOPUS y GLACY+*. 26-27 de noviembre de 2021.

Consejo de Europa. *Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018*. Estrasburgo, 9 de julio de 2018.

Consejo de Europa. *Estrategia de Igualdad de Género 2018-2023*. Madrid, Ministerio de Asuntos Exteriores y de Cooperación, 2018.

Consejo de Europa. *Proteger a las mujeres y niñas de la violencia en la era digital. La relevancia del Convenio de Estambul y del Convenio de Budapest sobre la Ciberdelincuencia para luchar contra la violencia contra las mujeres en línea y facilitada por la tecnología*. Octubre de 2021.

Consejo de Europa. *Recomendación CM/Rec 2019 del Comité de Ministros a los Estados miembros para prevenir y combatir el sexismo*. Adoptada por el Comité de Ministros el 27 de marzo de 2019 en la reunión n.º 1342 de los delegados de los ministros.

Consejo de Europa. *Segundo Protocolo adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas*. Estrasburgo, 12 de mayo de 2022.

Consejo de la Unión Europea. *Conclusiones del Consejo sobre la alfabetización mediática en un mundo en constante transformación (2020/C 193/06)*. Diario Oficial de la Unión Europea, 9 de junio de 2020.

Consejo de la Unión Europea. *Recomendación (UE) 2021/1004 del Consejo de 14 de junio de 2021 por la que se establece una garantía infantil europea*. Diario Oficial de la Unión Europea, de 22 de junio de 2021.

Diputación de Granada. Delegación de Igualdad, Juventud y Administración Electrónica. *Ni zorras ni héroes. Guía para trabajar el consumo de pornografía en menores. Conceptos básicos y actividades para llevar a cabo con grupos de adolescentes o en tutorías educativas*. Diputación de Granada. Delegación de Igualdad, Juventud y Administración Electrónica, Granada, 2021.

Federación de Mujeres Progresistas. *Guía informativa sobre ciberviolencias y delitos de odio por razón de género*. Federación de Mujeres Progresistas, Madrid, 24 de abril de 2020.

Federación de Mujeres Progresistas. *Trata de Mujeres con fines de explotación sexual en España*. Federación de Mujeres Progresistas, Madrid, 2008.

Fiscalía General del Estado. *Circular 1/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre disposiciones comunes y medidas de aseguramiento de las diligencias de investigación tecnológica en la LECRIM*. Madrid: FGE, 2019.

Fiscalía General del Estado. *Circular 2/2015, de 19 de junio, sobre los delitos de pornografía infantil tras la reforma operada por LO 1/2015*. Madrid: FGE, 2015.

Fiscalía General del Estado. *Circular 2/2019, de 6 de marzo, de la Fiscalía General del Estado, sobre interceptación de comunicaciones telefónicas y telemáticas*. Madrid: FGE, 2019.

Fiscalía General del Estado. *Circular 3/2017, de 21 de septiembre, sobre la reforma del Código Penal operada por la LO 1/2015, de 30 de marzo, en relación con los delitos de descubrimiento y revelación de secretos y los delitos de daños informáticos*. Madrid: FGE, 2017.

Fiscalía General del Estado. *Circular 3/2019, de 6 de marzo, de Fiscalía General del Estado, sobre captación y grabación de comunicaciones orales mediante utilización de dispositivos electrónicos*. Madrid: FGE, 2019.

Fiscalía General del Estado. *Circular 4/2019, de 6 de marzo, de Fiscalía General del Estado, sobre utilización de dispositivos técnicos de captación de imagen, de seguimiento y localización*. Madrid: FGE, 2019.

Fiscalía General del Estado. *Circular 5/2019, de 6 de marzo, de Fiscalía General del Estado, sobre registro de dispositivos y equipos informáticos*. Madrid: FGE, 2019.

Fundación Anesvad. *Informe sobre la pornografía infantil en Internet*. ANESVAD, 2003.

Grupo de Expertos en la Lucha contra la Violencia contra la Mujer y la Violencia Doméstica (GREVIO). *Primer Informe de evaluación de GREVIO sobre las medidas legislativas y de otra índole que dan efecto a las disposiciones del Convenio del Consejo de Europa sobre Prevención y Lucha contra la violencia contra las Mujeres y la Violencia Doméstica (Convenio de Estambul) ESPAÑA*. 2019.

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 la mujer*. 20 de octubre de 2021.

Grupo de Expertos sobre la Lucha contra la Trata de Seres Humanos (GRETA). *Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by Spain*. 2018.

Institut Balear de la Dona (IBD); Universitat de les Illes Balears (UIB). *Estudio sobre pornografía en las Illes Balears: acceso e impacto sobre la adolescencia, derecho internacional y nacional aplicable y soluciones tecnológicas de control y bloqueo*. IBD-UIB, Islas Baleares, 2022.

Instituto Europeo de la Igualdad de Género. *La ciberviolencia contra mujeres y niñas*. Instituto Europeo de la Igualdad de Género, 2022.

Instituto Nacional de Estadística (INE). *Equipamiento y uso de TIC en los hogares año 2023*. INE, 2023.

Instituto Nacional de Estadística (INE). *Estadística de Condenados: Adultos / Estadística de Condenados: Menores, año 2022*. INE, 2022.

Interactive Advertising Bureau Spain (IAB). *Estudio de Redes Sociales, 2023*. IAB, 2023.

LLORIA GARCÍA, P.; *«Por qué la difusión de imágenes sexuales en plataformas online sin el consentimiento de las personas que aparecen en ellas es delito»*. Maldita.es, 20 de junio de 2022.

LLORIA GARCÍA, P.; *«Sexting y sextorsión: dos modalidades delictivas con sesgo de género»,* en ibericonnect.blog, 2023.

Lobby Europeo de Mujeres en España (LEM España). *Estudio sobre el impacto de la propuesta de Directiva de la Comisión Europea sobre violencia contra las mujeres*. LEM España, Madrid, 2022.

MAGRO SERVET, V.; *Los delitos de sexting (197.7) y stalking (172 ter) en la reforma del Código Penal*. 2015.

MESEGUER GONZÁLEZ, J.D.; *Pericias informáticas: Aspectos procesales penales*. ElDerecho.es, Tribuna, internet, 10 de septiembre de 2013.

Ministerio de Asuntos Económicos y Transformación Digital. *Carta de Derechos Digitales española*. Madrid: Ministerio de Asuntos Económicos y Transformación Digital, 24 de julio 2011.

Ministerio de Asuntos Económicos y Transformación Digital. Observatorio Nacional de Tecnología y Sociedad. *Violencia de género: una realidad invisible*. Madrid: Observatorio Nacional de Tecnología y Sociedad, 2022.

Ministerio de Derechos Sociales y Agenda 2030. Instituto de la Juventud (INJUVE). *Violencia de género en la juventud. Las mil caras de la violencia machista en la población joven*. Revista de Estudios de Juventud n. 125. Madrid: INJUVE, marzo de 2022.

Ministerio de Igualdad. Delegación del Gobierno contra la Violencia de Género. *Macroencuesta de Violencia contra la Mujer 2019*. Madrid: Ministerio de Igualdad, 2019.

Ministerio de Industria, Energía y Turismo, a través de Red.es, la Sociedad Española de Medicina del Adolescente (SEMA) y el Hospital Universitario La Paz. *Guía clínica sobre el ciberacoso para profesionales de la salud*. Madrid: Ministerio de Industria, Energía y Turismo, marzo 2015.

Ministerio de Sanidad, Servicios Sociales e Igualdad. Delegación del Gobierno contra la Violencia de género. *El ciberacoso como forma de ejercer la violencia de género en la juventud: un riesgo en la sociedad de la información y del conocimiento*. Madrid: Ministerio de Sanidad, Servicios Sociales e Igualdad, 2014.

Observatorio de la Seguridad de la Información de INTECO y por Pantallas Amigas. *Guía sobre adolescencia y sexting: qué es y cómo prevenirlo*. Observatorio de la Seguridad de la Información, febrero, 2011.

ONU. *Informe ciberviolencia y ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará*. ONU Mujeres. 2022.

ONU. *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*. Consejo de Derechos Humanos, 38º período de sesiones, de 18 de junio a 6 de julio de 2018.

ONU. Comisión de Banda Ancha para el Desarrollo Sostenible. *Combatir la ciberviolencia contra las mujeres y las niñas: Una llamada de atención al mundo*. ONU, 2015.

ONU. *La prostitución y la violencia contra las mujeres y las niñas. Informe de la Relatora especial sobre la violencia contra las mujeres y las niñas, sus causas y consecuencias, Reem Alsalem*. Consejo de Derechos Humanos, 56º período de sesiones, 18 de junio a 12 de julio de 2024.

Organización de los Estados Americanos (OEA)-Comité Interamericano Contra el Terrorismo; OEA-Comisión Interamericana de Mujeres. *La violencia de género en línea contra las mujeres y niñas, Guía de conceptos básicos*. OEA, marzo, 2022.

PALOMO, Roberto. «*Un año de libertad vigilada para 15 menores de Almendralejo por manipular imágenes de niñas*», ElPaís.es, 2023.

PÉREZ RIQUELME, A.; *La prueba digital. Naturaleza, admisibilidad, impugnación y valoración*. Paréntesis Legal, 14 de noviembre 2021.

Plan International España. *(In)seguras online: Resultados de España*. Plan Internacional, 2020.

Radio Televisión Española (RTVE). «*Mi hijo no ve porno». Documental del programa «En portada*». Guionistas: Isabel Ojeda, Alicia Gómez Sánchez. Dirigido por: Teresa Martín. RTVE, 23 de noviembre de 2023.

Recomendación general núm. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19 del Comité para la Eliminación de la Discriminación contra la Mujer (CEDAW), ONU, de 26 de julio de 2017.

Recomendación (UE) 2018/334 de la Comisión, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea. Diario Oficial de la Unión Europea núm. 63, de 6 de marzo de 2018.

RODRÍGUEZ ACOSTA, M.; *La prueba digital en el proceso penal*. Trabajo fin de máster. Ilustre Colegio de Abogados de Santa Cruz de Tenerife, Escuela de Práctica Jurídica Santa Cruz de Tenerife y Universidad La Laguna. Santa Cruz de Tenerife, 19 de enero de 2018.

Save the Children. *(Des)información Sexual: pornografía y adolescencia*. Save the Children España, junio 2020.

Save the Children. *Violencia viral. Resumen ejecutivo*. Save the Children, julio 2019.

Security Hero, State of deepfakes. *Realities, Threats, and Impact*. 2023.

Sociedad Española de Psicología Jurídica y Forense. *XIV Congreso (INTER)nacional de psicología jurídica y forense. Libro de actas*. Sociedad Española de Psicología Jurídica y Forense, Santiago de Compostela, noviembre 2022.

UNHCR ACNUR. *Guía metodológica sobre violencia de género digital. Dirigida a equipos de atención a personas en movilidad humana. Taller de comunicación mujer*. UNHCR ACNUR, Quito, febrero 2022.

VALENCIA RODRÍGUEZ, N.; *Pornografía virtual infantil*. Trabajo de Fin de Grado. Universidad Autónoma de Barcelona. Barcelona, 18 de agosto de 2014.

VELASCO NÚÑEZ, E.; *Novedades técnicas de investigación penal vinculadas a las nuevas tecnologías*. ElDerecho.es, Tribuna, penal, 24 de febrero 2011.

Referencias jurisprudenciales

Tribunal Supremo de Estados Unidos, sentencia 25 junio 2014, (casos acumulados Riley contra California y Estados Unidos contra Brima Wurie-573 U.S.-2014)

Tribunal Europeo de Derechos Humanos

STEDH de 22 de mayo de 2008, caso Iliya Stefanov contra Bulgaria.

STEDH, de 7 de enero de 2010, asunto Rantsev c. Chipre y Rusia (Demanda 25965/04).

Tribunal Constitucional

STC núm. 114/1984, de 21 de diciembre, Rec. 167-1984.

Tribunal Supremo

STS núm. 105/2009, Sala 2ª, de lo Penal, de 30 de enero, Rec. 1358/2008.

STS núm. 795/2009, Sala 2ª, de lo Penal, de 28 de mayo, Rec. 11466/2008.

STS núm. 271/2012, Sala 2ª, de lo Penal, de 26 de marzo, Rec. 1605/2012.

STS núm. 97/2015, Sala 2ª, de lo Penal, de 24 de febrero, Rec. 1774/2014.

STS núm. 300/2015, Sala 2ª, de lo Penal, de 19 de mayo, Rec. 2387/2014.

STS núm. 527/2015, Sala 2ª, de lo Penal, de 22 de septiembre, Rec. 294/2015.

STS núm. 864/2015, Sala 2ª, de lo Penal, de 10 de diciembre, Rec. 912/2015.

STS núm. 988/2016, Sala 2ª, de lo Penal, de 11 de enero, Rec. 10342/2016.

STS núm. 301/2016, Sala 2ª, de lo Penal, de 12 de abril, Rec. 1229/2015.

STS núm. 109/2017, Sala 2ª, de lo Penal, de 22 de febrero, Rec. 10439/2016.

STS núm. 324/2017, Sala 2ª, de lo Penal, de 8 de mayo, Rec. 1775/2016.

STS núm. 554/2017, Sala 2ª, de lo Penal, de 12 de julio, Rec. 1745/2016.

STS núm. 72/2018, Sala 2ª, de lo Penal, de 9 de febrero, Rec. 583/2017.

STS núm. 377/2018, Sala 2ª, de lo Penal, de 23 de julio, Rec. 10036/2018.

STS núm. 450/2018, Sala 2ª, de lo Penal, de 10 de octubre, Rec. 2547/2017.

STS núm. 70/2020, Sala 2ª, de lo Penal, de 24 de febrero, Rec. 3335/2018.

STS núm. 37/2021, Sala 2ª, de lo Penal, de 21 de enero, Rec. 1074/2019.

STS núm. 395/2021, Sala 2ª, de lo Penal, de 6 de mayo, Rec. 10258/2020.

STS núm. 447/2021, Sala 2ª, de lo Penal, de 26 de mayo, Rec. 3097/2019.

STS núm. 843/2021, Sala 2ª, de lo Penal, de 4 de noviembre, Rec. 4682/2019.

STS núm. 916/2021, Sala 2ª, de lo Penal, de 24 de noviembre, Rec. 5415/2019.

STS núm. 61/2022, Sala 2ª, de lo Penal, de 26 de enero, Rec. 609/2020.

STS núm. 699/2022, Sala 2ª, de lo Penal, de 11 de julio, Rec. 3204/2020.

STS núm. 871/2022, Sala 2ª, de lo Penal, de 7 de noviembre, Rec. 10258/2022.

STS núm. 995/2022, Sala 2ª, de lo Penal, de 22 de diciembre, Rec. 10375/2022.

STS núm. 15/2023, Sala 2ª, de lo Penal, de 19 de enero, Rec. 4891/2020.

STS núm. 181/2023, Sala 2ª, de lo Penal, de 15 de marzo, Rec. 3337/2021.

STS núm. 767/2023, Sala 2ª, de lo Penal, de 3 de octubre, Rec. 5039/2021.

STS núm. 960/2023, Sala 2ª, de lo Penal, de 21 de diciembre, Rec. 744/2021.

STS núm. 325/2023, Sala 2ª, de lo Penal, de 10 de mayo, Rec. 10736/2022.

STS núm. 376/2023, Sala 2ª, de lo Penal, de 18 de mayo, Rec. 10566/2022.

STS núm. 494/2023, Sala 2ª, de lo Penal, de 22 de junio, Rec. 3986/2021.

STS núm. 297/2024, Sala 2ª, de lo Penal, de 3 de abril, Rec. 1041/2022.

STS núm. 416/2024, Sala 2ª, de lo Penal, de 16 de mayo, Rec. 5543/2023

STS núm. 476/2024, Sala 2ª, de lo Penal, de 23 de mayo, Rec. 1017/2022.

STS núm. 716/2024, Sala 2ª, de lo Penal, de 4 de julio, Rec. 10029/2024.

Audiencias provinciales

SAP de Madrid núm. 489/2009, Sección 3, de 16 de noviembre, Rec. 62/2009.

SAP de Madrid núm. 313/2014, Sección 27, de 22 de mayo, Rec. 779/2014.

SAP de Tarragona núm. 135/2015, Sección 2, de 8 de abril, Rec. 18/2013.

SAP de Albacete núm. 221/2015, Sección 1, de 22 de septiembre, Rec. 2/2014.

SAP de Vizcaya núm. 17/2017, Sección 2, de 7 de abril, Rec. 59/2015.

SAP de Madrid núm. 705/2018, Sección 30, de 18 de octubre, Rec. 73/2018.

SAP de Madrid núm. 716/2018, Sección 29, de 12 de diciembre, Rec. 1397/2018.

SAP de Barcelona núm. 75/2020, Sección 8, de 3 de febrero, Rec. 10/2019.

SAP de Badajoz núm. 130/2020, Sección 3, de 1 de octubre, Rec. 6/2019.

SAP de Tarragona núm. 463/2021, Sección 2, de 25 de noviembre, Rec. 16/2021.

SAP de Málaga núm. 106/2022, Sección 2, de 31 de marzo, Rec. 37/2019.

SAP de Santa Cruz de Tenerife núm. 247/2022, Sección 6, de 15 de junio, Rec. 46/2021.

SAP de Ceuta núm. 51/2022, Sección 6, de 27 de junio, Rec. 23/2021.

SAP de Barcelona núm. 138/2023, Sección 5, de 1 de marzo, Rec. 30/2020.

SAP de Madrid núm. 117/2023, Sección 17, de 8 de marzo, Rec. 623/2022.

SAP de Toledo núm. 31/2023, Sección 2, de 15 de marzo, Rec. 53/2021.

SAP de Álava núm. 103/2023, Sección 2, de 2 de mayo, Rec. 40/2022.

SAP de Salamanca núm. 23/2023, Sección 1, de 22 de junio, Rec. 9/2023.

SAP de Madrid núm. 7/2024, Sección 27, de 10 de enero, Rec. 1775/2023.

SAP de Barcelona núm. 301/2024, Sección 22, de 21 de marzo, Rec. 11/2024.

SAP de Almería núm. 290/2024, Sección 3, de 5 de junio, Rec. 186/2024.