



**Cooperación
Española**

CONOCIMIENTO / INTERCOONECTA

Curso de Especialización Judicial

Ciberdelincuencia: tratamiento preventivo, procesal y sustantivo desde una perspectiva internacional. 4ª Edición

Autor,
Zita Hernández Larrañaga

Cargo **Magistrado**

Institución **CGPJ**

País **ESPAÑA**



Consejo General
del Poder Judicial
Escuela Judicial

Aula

Iberoamericana

Consejo General del Poder Judicial



CIBERDELINCUENCIA DE GENERO

CYBER VAWG

VIOLENCIA EN LÍNEA CONTRA LA MUJER

VIOLENCIA CONTRA LAS MUJERES EN SU DIMENSIÓN DIGITAL



DEFINICIÓN

- No existe una definición establecida de manera uniforme, ni a nivel nacional ni a nivel internacional
- La Relatora Especial de las Naciones Unidas define la «violencia en línea contra las mujeres» como todo acto de violencia de género contra las mujeres cometido, asistido o agravado en parte o en su totalidad por el uso de las TIC, como los teléfonos móviles y teléfonos inteligentes, internet, las plataformas de redes sociales o el correo electrónico, contra una mujer por su condición de mujer, o que afecte a las mujeres de manera desproporcionada” – Informe acerca de la violencia en línea contra mujeres y niñas desde la perspectiva de los DDHH 18 de junio de 2018

-
- También puede verificarse en o a través de una gran variedad de plataformas de internet, como por ejemplo: redes sociales (Facebook, Instagram, Twitter, Tik Tok, Snapchat), servicios de correo electrónico, aplicaciones de mensajería instantánea (Whatsapp o Messenger), aplicaciones de citas (Tinder, Grindr, Hinge, Match.com) videojuegos en línea, sitios donde se intercambia contenido (Reddit), foros de discusión en línea, en las secciones de comentarios de los periódicos, o en plataformas generadas por personas usuarias (wikis, blogs, sitios para intercambio de imágenes y videos), entre otras.
 - Permitir terminos abiertos, dinamicos y genericos, que incluya una amplia gama de conductas con perspectiva de género .

-
- Consejo Europa – Convenio de Estambul GREVIO – RECOMENDACIÓN general nº I sobre la dimensión digital de la violencia contra las mujeres adoptada el 20 de octubre de 2021 considera que el término "violencia contra las mujeres en su dimensión digital" o "la dimensión digital de la violencia contra las mujeres" es lo suficientemente amplio como para abarcar tanto los actos de violencia en línea como los perpetrados a través de la tecnología, incluida la tecnología aún por desarrollar.
 - Complementario - el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) -ofrece un amplio conjunto de normas jurídicamente vinculantes para tipificar como delito aspectos de la ciberviolencia, obtener pruebas y entablar una cooperación transfronteriza e internacional para investigar y también perseguir la violencia en línea contra las mujeres.
 - El caso Buturugă contra Rumanía -primer reconocimiento explícito de la ciberviolencia por parte del Tribunal Europeo de Derechos Humanos.

-
- Estrategia para la Igualdad de Género 2020-2025 de la Unión Europea (presentada por la Comisión Europea como herramienta para combatir la violencia contra las mujeres en toda su diversidad y la violencia de género, y abordar sus causas profundas) subraya que la ciberviolencia de género está profundamente arraigada en la dinámica el poder, los desequilibrios económicos y las normas de género; pide a los Estados miembros y a la Comisión que aborden las causas profundas de la ciberviolencia de género y que combatan los roles de género y los estereotipos establecidos que hacen que la violencia contra las mujeres sea aceptable
 - La ciberviolencia de género no es una nueva forma de violencia, sino una extensión (manifestación) de la violencia de género, y su finalidad es controlar y atacar a las mujeres y mantener y reforzar las normas, los papeles y las estructuras patriarcales, y una relación de poder desigual.

-
- La protección de los derechos humanos de la mujer y la eliminación de la violencia contra las mujeres y las niñas en la vida pública y privada en el “mundo real” sigue siendo un reto mundial que se ha extendido al espacio digital de los medios sociales.
 - La interacción entre la tecnología y las normas de derechos humanos de la mujer se caracteriza por el reconocimiento del principio de que los derechos de las personas también deben estar protegidos en Internet. Habida cuenta de que los derechos de la mujer son derechos humanos y la prohibición de la violencia de género se ha reconocido como un principio del derecho internacional de los derechos humanos, los derechos humanos de la mujer amparados mediante convenciones, jurisprudencia y normas amplias regionales e internacionales deben estar protegidos en Internet, en particular mediante la prohibición de la violencia por razón de género en formas facilitadas por las TIC y en línea.

DATOS SOBRE CIBERDELINCUENCIA A NIVEL INTERNACIONAL

- Servicio de Estudios del Parlamento Europeo 2014 (La Lucha contra la violencia de género: la ciberviolencia – Evaluación del valor añadido europeo)sobre ciberviolencia de género:
 - estima que entre el 4 y el 7 % de las mujeres de la Unión ha sido víctima de ciberacoso durante los 12 meses anteriores al estudio, mientras que entre el 1 y el 3 % ha sufrido ciberhostigamiento.
 - el 23% de las mujeres manifestaron haber sufrido abuso o acoso en línea al menos una vez en su vida, y que 1 de cada 10 mujeres ha sido víctima de alguna forma de violencia en línea desde los 15 años de edad.

-
- La Comisión de Banda Ancha de las Naciones Unidas señaló en 2015 que la violencia de género contra las mujeres y las niñas había alcanzado proporciones pandémicas también en internet, identificando que 73% de las mujeres había experimentado alguna forma de violencia en línea, mientras que 61% de los acosadores en línea se habían identificado como hombres.
 - En el informe titulado Toxic Twitter. A Toxic Place for Women, Amnistía Internacional (AI) 2018 subrayó que 88% de las mujeres encuestadas había sufrido acoso u hostigamiento al utilizar Twitter para abordar temáticas feministas o vinculadas a la igualdad de género.

WORDL WIDE WEB FOUNDATION

La encuesta realizada en 2020 con participantes de 180 países reveló que el 52 % de las mujeres jóvenes y niñas ha sufrido abusos en línea, como el intercambio de imágenes, vídeos o mensajes privados sin consentimiento, mensajes de odio y humillantes, lenguaje injurioso y amenazante, acoso sexual y contenidos falsos, y que el 64 % de los encuestados afirmó conocer a alguien que los ha sufrido

ENCUESTA DE LA DELEGACIÓN CONTRA LA VIGE

- Encuesta 2019 10.000 participantes
- El 7,4% de las de 16 o más años ha recibido alguna vez insinuaciones inapropiadas, humillantes, intimidatorias u ofensivas a través de las redes sociales. Si se tienen en cuenta las que han experimentado algún tipo de acoso sexual, el 18,4%habría sufrido dicho acoso a través de las redes sociales..

-
- Los costes totales del ciberacoso y del ciberhostigamiento oscilan entre los 49 000 y los 89 300 millones EUR e indica que la mayor categoría de costes corresponde al valor de la pérdida de calidad de vida, que representa más de la mitad de los costes totales (alrededor del 60 % en el caso del ciberacoso y en torno al 50 % en el caso del ciberhostigamiento)

CARACTERISTICAS



- En el marco de una relación interpersonal, incluyendo relaciones familiares, sexo-afectivas o de pareja.
- Puede estar vinculada o ser una expresión de la violencia de género que tiene lugar en la comunidad, como por ejemplo en el ámbito educativo tomando la forma de ciberbullying basado en el género, o en el lugar de trabajo como ciberhostigamiento sexual o ciberacoso laboral (cibermobbing)
- Puede ser perpetrada por cualquier persona en el contexto de las interacciones de la comunidad digital desarrolladas en las plataforma de internet, como es el caso de actos de ciberacoso en redes sociales por parte de usuarios de internet desconocidos
- Puede ser cometida o tolerada por el Estado o sus agentes.

-
- El anonimato que confiere a los autores, pero el 40% de las víctimas conocen al agresor y en un tercio de los casos, tenían o habían tenido una relación íntima – informe APC
 - Puede llevarse a cabo desde cualquier lugar y escala y de modo indeleble.
 - Tiene un carácter multijurisdiccional y transnacional, dado que muchos de los actos de abuso se cometen fuera de la jurisdicción de los Estados.
 - *Continuum* de la violencia de género fuera y dentro del internet.
 - Amplia variedad de prácticas
 - No es un fenómeno aislado, sino que es parte de un contexto de discriminación por motivos de género y de violencia sistémica contra las mujeres y niñas

-
- Nuevo espacio para contenidos y comportamientos agresivos y violentos nunca antes vistos
 - Su instantaneidad, rápida expansión, (viralización), su permanencia y registro digital
 - Indeleble, su replicabilidad y alcance global, y la posibilidad de localizar fácilmente a las víctimas y revictimizarlas mientras el agresor o los agresores permanecen en el anonimato.
 - Afecta a los derechos fundamentales de mujeres y niñas (vida libre de violencia, integridad física, psíquica y moral, libertad y seguridad, dignidad, igualdad, libertad de reunión y expresión, privacidad, libertad sexual)

MODALIDADES

THE BROADBAND COMMISSION FOR DIGITAL DEVELOPMENT WAS LAUNCHED BY THE INTERNATIONAL TELECOMMUNICATION UNION (ITU) AND THE UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION (UNESCO) 2015

- **Hacking:** el uso de la tecnología para obtener acceso ilegal o no autorizado a sistemas o el propósito de adquirir información personal, alterar o modificar información, o difamar, calumniar y denigrar a la víctima y/o a las organizaciones de lucha contra la violencia de género. Por ejemplo, violación de contraseñas y control de funciones informáticas, como congela el ordenador o cerrar la sesión del usuario
- **Suplantación de identidad:** uso de la tecnología para la identidad de la víctima o de otra persona para acceder a información privada, avergonzar a la víctima, contactar con ella o crear documentos de identidad fraudulentos; por ejemplo, enviar correos electrónicos ofensivos desde la cuenta de correo electrónico de la víctima; llamar a la víctima desde un número desconocido para evitar que la llamada sea bloqueada.



-
- **3. Vigilancia/seguimiento:** el uso de la tecnología para acechar y controlar las actividades y comportamientos de la víctima, ya sea en tiempo real o pasado. Ej. seguimiento GPS a través del teléfono móvil.
 - **4. Acoso/Spamming:** el uso de la tecnología para contactar continuamente, molestar, amenazar y/asustar a la víctima. Se trata de un comportamiento continuado y no de un incidente aislado; p. ej., llamadas persistentes a móviles/mensajes de texto; llenar el buzón de voz de mensajes para que nadie más pueda dejar un mensaje.

-
- **5. Captación:** uso de la tecnología para atraer a víctimas potenciales a situaciones violentas.fraudulentos (sitios de citas;oportunidades de empleo); los traficantes utilizan chats, tableros de anuncios y sitios web para comunicarse/anunciarse
 - **6. Distribución maliciosa:** uso de la tecnología para manipular y distribuir material difamatorio e ilegal relacionados con la víctima y/organizaciones; por ejemplo, amenazar o filtrar fotos/vídeos íntimos; uso de la tecnología como herramienta de propaganda para promover la violencia contralas mujeres.

- **CIBERHOSTIGAMIENTO – CIBERACECHO**

- Comisión reiterada por la comisión reiterada por parte de una misma persona, de actos abusivos y perturbadores a través del uso de las TIC, con el objetivo de hostigar, intimidar, acechar, molestar, controlar, atacar, humillar, amenazar, asustar, ofender o abusar verbalmente a una víctima.
- Contextos de violencia doméstica y pareja
- Extensible a familiares, amigos o nuevas parejas de la víctima

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

INFORME ONU MUJERES – OFICINA REGIONAL PARA AMÉRICA LATINA Y EL CARIBE – Y EL MECANISMO DE SEGUIMIENTO DE LA CONVENCIÓN BELÉM DO PARÁ (MESECVI) DE LA COMISIÓN INTERAMERICANA DE MUJERES 2021

• CIBERACOSO

- Gran variedad de manifestaciones: abusar, humillar, molestar, atacar, amenazar, degradar, intimidar ofender y/o insultar a una persona por razones de género, creando un ambiente ofensivo y hostil en los espacios digitales.

Basta la existencia de un solo incidente para que éste se verifique (si bien puede estar conformado por diversos incidentes), y puede realizarse por múltiples agresores de forma coordinada o esporádica)

- Puede también dirigirse en contra de una mujer como parte de un ataque grupal, masivo-ciberturbas –cybermobs (muchas veces transfronterizo) y anónimo con el objetivo de humillarla o causarle angustia mediante campañas o estrategias coordinadas.



Doxing (GAMERGATE, Clara Sorrenti, víctima Manada)

Cyberflashing (el acto de enviar imágenes obscenas no solicitadas), gendertrolling (publicación de contenido extremadamente ofensivo y hashtags en redes sociales para provocar efectos en la opinión pública e incitar a la violencia contra las mujeres)

Sealioning consiste en el acoso de una persona con solicitudes persistentes de evidencia, preguntas y/o invitaciones incesantes de involucrarse en un debate en línea con un pretendido sentido de sinceridad y civilidad, a fin de provocar una respuesta agresiva que pueda ser utilizada para contraatacar.



- **MATERIAL NATURALEZA SEXUAL O INTIMA SIN CONSENTIMIENTO**

- Existencia de material audiovisual (real o editado) de carácter íntimo y/o sexual;
- Creación, almacenamiento, manipulación producción, difusión, publicación, distribución, facilitación, cesión o entrega a terceros de este material
- Intermediación de las TIC
- Falta de consentimiento de la persona que aparece en ese material (bien para su creación u obtención, bien para su distribución)

-
- **Sextorsion**-amenaza con distribuir tu material privado y sensible si no le proporcionas imágenes de naturaleza sexual, favores sexuales o dinero.
 - **Porn-revenge/porno venganza**- compartir contenido sexual de ex pareja para humillarla
 - **Sexpreding**-el envío de fotografías de contenido sexual sin el consentimiento de la persona que aparece
 - **Creepshots**- hacer fotos de mujeres, en sitios públicos, sexualmente sugerentes y no explícitas y compartirlas en red
 - **Upskirting**- captar con cámara oculta a mujeres en "las zonas genitales" sin su consentimiento para después subir estos vídeos a la red

-
- Downblousing- lo mismo pero con la zona del pecho
 - Deepfake
 - Doxxing en web de anuncios de servicios sexuales

- **CONTROL O VIGILANCIA A DISTANCIA (TAMBIÉN A TRAVÉS DE APLICACIONES ESPÍA EN DISPOSITIVOS MÓVILES)**

- Rastreo de las actividades de la víctima, off line y on line
- Uso Internet de las Cosas
- Software espías
- Uso de cámaras
- Envío constante de geolocalización
- Obligar a compartir contraseñas
- Acceso ilícito a cuentas móviles, de correo electrónico, de mensajería instantánea o de redes sociales

-
- **AMENAZAS** (incluidas las amenazas directas y las amenazas de violencia, extorsión, sextorsión, chantaje)
 - **DISCURSO DE ODIO SEXISTA** (incluidos: publicar y compartir contenidos violentos, utilizar comentarios o insultos sexistas o de género e insultar a las mujeres por expresar sus propias opiniones y rechazar las insinuaciones sexuales),
 - **CONDUCTAS INDUCTORAS DEL SUICIDIO O LA ANOREXIA O LAS LESIONES PSÍQUICAS**

-
- **DAÑOS INFORMÁTICOS A ARCHIVOS, PROGRAMAS, DISPOSITIVOS Y ATAQUES A SITIOS WEB Y OTROS CANALES DE COMUNICACIÓN DIGITAL**
 - **INCUMPLIMIENTO DE LAS PROHIBICIONES DE COMUNICACIÓN ADOPTADAS POR RESOLUCIÓN JUDICIAL**
 - **SUPLANTACIÓN Y ROBO DE IDENTIDAD EN LINEA**
 - **ATAQUES A LA REPUTACIÓN O LA CREDIBILIDAD – GOOGLE BOMBING**
 - **VIOLENCIA DIRECTA – uso TIC para ubicar y localizar a la víctima a fin de atacarla**

-
- **EXPLOTACIÓN SEXUAL Y/O TRATA DE MUJERES Y NIÑAS**
 - **CIBERATAQUES A GRUPOS, ORGANIZACIONES, COMUNIDADES O COLECTIVOS DE MUJERES**
 - Ataques masivos
 - Uso trolls o bots

RECOMENDACIÓN NUMERO I GREVIO – CONVENIO DE ESTAMBUL

- Muchas de las formas de violencia contra las mujeres perpetradas a través de medios digitales entran en el ámbito de las conductas intencionadas, que los Estados Partes en el Convenio de Estambul deben tipificar como delito. Se trata de la violencia psicológica en línea (artículo 33), el acoso en línea o acecho cometido en el ámbito digital (artículo 34) y el acoso sexual en línea o a través de medios digitales (artículo 40).
- **Comportamientos que suponen acoso sexual en línea:**
 - 1) compartir imágenes o vídeos sin consentimiento El intercambio no consentido de imágenes (fotos o vídeos) de desnudos o de contenido sexual de una persona, o las amenazas de hacerlo, incluyen actos de abuso sexual basado en imágenes (también conocidos como "pornografía vengativa")

-
- 2) tomar, producir o procurar imágenes o vídeos íntimos sin consentimiento -incluye actos de "upskirting" y "creepshots", así como la producción de imágenes alteradas digitalmente en las que la cara o el cuerpo de una persona se superponen o "cosen" en una foto o vídeo pornográfico, lo que se conoce como "pornografía falsa" (como los "deepfakes", cuando se crean imágenes sintéticas utilizando inteligencia artificial)
 - 3) explotación, coacción y amenazas incluyen formas de violencia como el sexting forzado, la extorsión sexual, las amenazas de violación, el doxing sexualizado/género, la suplantación de identidad y el outing

-
- 4) Acoso sexualizado - comportamientos como hacer circular chismes o rumores sobre el supuesto comportamiento sexual de una víctima, publicar comentarios sexualizados en los mensajes o fotos de la víctima, suplantar la identidad de una víctima y compartir contenido sexual o acosar sexualmente a otras personas, afectando así a su reputación o a su medio de vida, o "sacar del armario" a alguien sin su consentimiento con el fin de asustar, amenazar y avergonzar.
 - 5) El cyberflashing - enviar imágenes sexuales no solicitadas a través de aplicaciones de citas o mensajería, mensajes de texto o mediante tecnologías Airdrop o Bluetooth.

Comportamientos que suponen acoso en línea- la conducta intencionada de realizar repetidamente conductas amenazadoras dirigidas a otra persona, haciéndola temer por su seguridad, mediante el uso de las TIC. Incluyen amenazas de índole sexual, económica, física o psicológica), daños a la reputación, seguimiento y recopilación de información privada sobre la víctima, usurpación de identidad, solicitud de sexo, suplantando la identidad de la víctima y acosándola con cómplices para aislarla. Suele implicar la táctica de vigilar o espiar a la víctima, en sus distintas redes sociales o plataformas de mensajería, sus correos electrónicos y teléfono ,robando contraseñas o crackeando o pirateando sus dispositivos para acceder a sus espacios privados, mediante la instalación de spyware o apps de geolocalización, o mediante el robo de sus dispositivos. Los autores también pueden asumir la identidad de la otra persona o vigilar a la víctima a través de dispositivos tecnológicos conectados mediante la Internet de las Cosas (IoT), como los electrodomésticos inteligentes.

-
- Como modalidad de violencia psicológica, en los foros digitales, el abuso económico puede manifestarse como el control de las cuentas bancarias y las actividades financieras de la víctima a través de la banca por Internet, dañando la calificación crediticia de la víctima mediante el uso de tarjetas de crédito sin permiso o presentando todos los contratos financieros (arrendamientos, préstamos, servicios públicos, etc.) a nombre de la víctima.

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

- Difusión no consentida de material íntimo o manipulado
- a) hacer accesible al público, mediante tecnologías de la información y de las comunicaciones (TIC), imágenes, vídeos o materiales similares que representen actividades sexualmente explícitas o las partes íntimas de una persona sin su consentimiento, cuando sea probable que tal conducta cause graves daños a esa persona;
- b) producir, manipular o alterar y, posteriormente, hacer accesible al público, mediante TIC, imágenes, vídeos o materiales similares, haciendo que parezca que una persona está practicando actividades sexualmente explícitas, sin el consentimiento de dicha persona, cuando sea probable que tal conducta cause graves daños a esa persona;
- c) amenazar con cometer las conductas mencionadas en las letras a) o b) con el fin de coaccionar a una persona para que realice o acceda a que se realice determinado acto o se abstenga de realizarlo.



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

-
- Ciberacoso
 - a) la participación reiterada o continua en conductas amenazantes dirigidas contra otra persona, al menos cuando esa conducta implique amenazas de cometer delitos, mediante TIC, y cuando sea probable que cause en la persona un profundo temor por su propia seguridad o por la seguridad de las personas a cargo;
 - b) la participación, junto con otras personas, mediante TIC, en conductas amenazantes o insultantes accesibles públicamente dirigidas contra una persona, cuando sea probable que tal conducta cause graves daños psicológicos a esa persona;
 - c) el envío no solicitado a una persona, mediante TIC, de una imagen, vídeo u otro material similar que represente los genitales, cuando sea probable que tal conducta cause daños psicológicos a esa persona;
 - d) hacer accesible al público, mediante TIC, material que contenga los datos personales de una persona, sin su consentimiento, con el fin de incitar a terceros a causar lesiones físicas o psicológicas graves a dicha persona.

REGULACION PENAL A NIVEL NACIONAL ESPAÑA

- Hasta el año 2015 se regulaba el delito de descubrimiento y revelación de secretos (197 CP) pero tal precepto exigía un acceso ilícito a las imágenes, vídeos o documentos (se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación)
- Delito contra la integridad moral (El que infligiera a otra persona un trato degradante, menoscabando gravemente su integridad moral)
- La mayoría de supuestos se tipificaban como coacciones y/o amenazas, o directamente eran archivados al considerar que la conducta no estaba tipificada

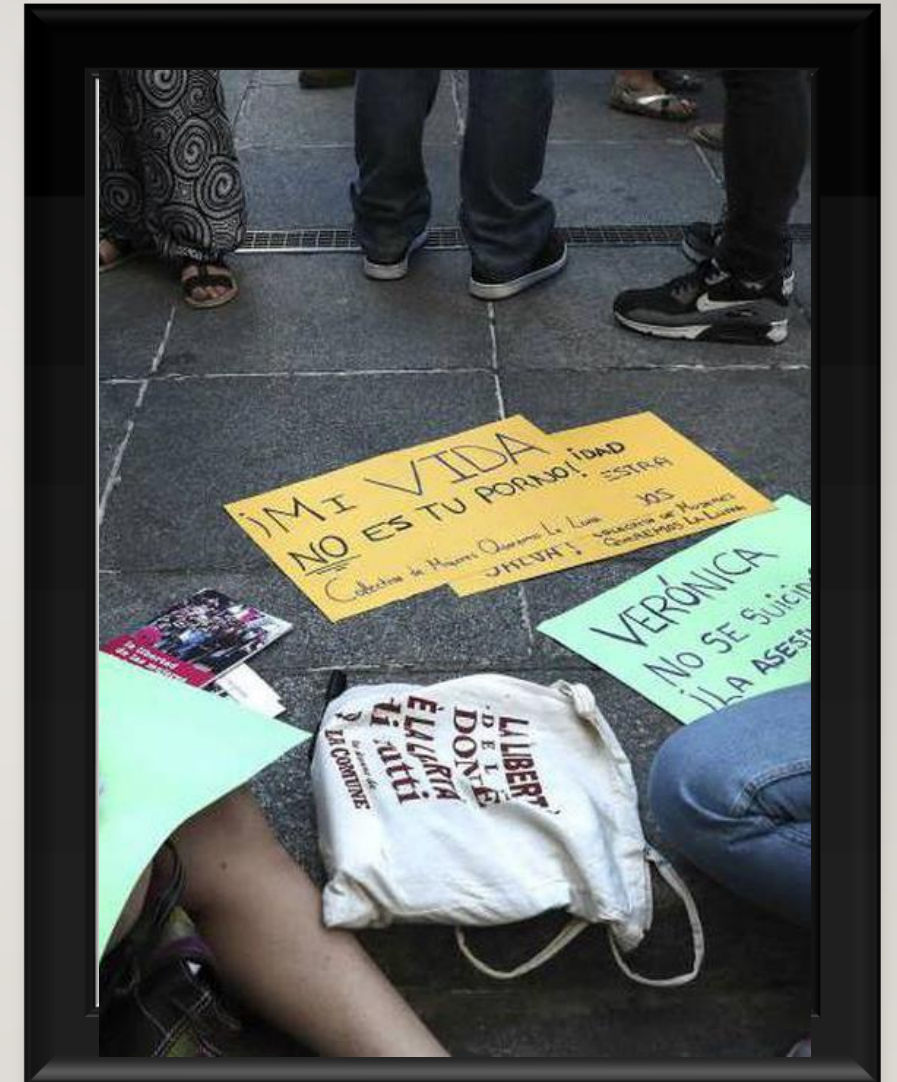
EN EL AÑO 2012- CASO OLVIDO HORMIGOS

Concejala de una localidad de Toledo y se difundió un vídeo íntimo que la llevó a dimitir de sus funciones. Denunció pero la denuncia fue archiva al considerar el juez que el video no se había obtenido de manera ilícita



EN EL AÑO 2019 – CASO IVECO

Difusion de un vídeo de contenido sexual de una trabajadora de la fabrica Iveco entre una plantilla formada por 2.500 trabajadores. La empresa no activó protocolo alguno para detener los múltiples reenvios del vídeo y en fecha 25 de mayo de 2019 la trabajadora se suicidó. Los hechos fueron denunciados pero nunca se pudo determinar quien havia realizado el primer envio y no havia denuncia de la víctima (estaba muerta)



-
- Ambos casos fueron muy mediáticos y provocaron cambios legislativos,
 - Serie de netflix basada en los mismos
 - LO 1/2015 y LO 10/2022 introducen preceptos que tipifican expresamente algunas de las modalidades mencionadas:



INTIMIDAD

Artículo 197.7 . Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona.

Se impondrá la pena de multa de uno a tres meses a quien 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.

En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior 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, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.

Requiere denuncia persona agraviada

El Tribunal Supremo se pronuncia por primera vez sobre el artículo 197.7 CP en febrero de 2020.



Artículo 172 ter.

1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de esta forma, altere el normal desarrollo de su vida cotidiana:

1.^a La vigile, la persiga o busque su cercanía física.

2.^a Establezca o intente establecer contacto con ella **a través de cualquier medio de comunicación**, o por medio de terceras personas.

3.^a Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.

4.^a Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella. Cuando la víctima se halle en una situación de especial vulnerabilidad por razón de su edad, enfermedad, discapacidad o por cualquier otra circunstancia, se impondrá la pena de prisión de seis meses a dos años.

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



-
- Art. 173.4 Las mismas penas se impondrán a quienes se dirijan a otra persona con expresiones, comportamientos o proposiciones de carácter sexual que creen a la víctima una situación objetivamente humillante, hostil o intimidatoria, sin llegar a constituir otros delitos de mayor gravedad.



-
- Mujeres víctimas de violencia íntima o de pareja
 - Mujeres víctimas o sobrevivientes de violencia física o sexual
 - Mujeres jóvenes: entre los 18 y 24 años enfrentan niveles más elevados de violencia en línea, con un 27% más de probabilidades con los hombres.
 - Mujeres con un perfil público o participantes activas de los debates digitales
 - Activistas y defensoras de los derechos humanos de las mujeres y LGBTQ+, mujeres identificadas como feministas, defensoras de la igualdad de género y activistas en el ámbito de la salud sexual y reproductiva.
 - Mujeres con discapacidad;
 - Integrantes de la comunidad LGBTQ+
 - Mujeres pertenecientes a minorías étnicas, mujeres indígenas, negras o afrodescendientes, racializadas y mujeres pertenecientes a colectivos marginalizados que defienden públicamente su identidad, corporalidad u origen.

BIBLIOGRAFIA

- Cyber Violence against Women and Girls: A world-wide wake-up call October 23, 2015 ITU/UNESCO Broadband Commission for Sustainable Development
- 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 - ONU
- Informe Ciber violencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará- 2021 ONU Mujeres – Oficina Regional para América Latina y el Caribe – y el Mecanismo de Seguimiento de la Convención Belém do Pará (MESECVI) de la Comisión Interamericana de Mujeres

-
- Mapping study on cyberviolence - Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children 2018 – Consejo de Europa
 - GREVIO General Recommendation No. 1 on the digital dimension of violence against women 2021 – Consejo de Europa
 - Cyber violence against women and girls 2017 - European Institute for Gender Equality
 - Combating Cyber Violence against Women and Girls 2022 -European Institute for Gender Equality

-
- Resolución del Parlamento Europeo, con recomendaciones destinadas a la Comisión sobre la lucha contra la violencia de género: la ciberviolencia 2021, Unión Europea