Introducción a la cibervictimización

PID_00270861

Irene Montiel Juan

Tiempo mínimo de dedicación recomendado: 2 horas

Universitat Oberta de Catalunya

Irene Montiel Juan

Doctora en Psicología, criminóloga y psicóloga jurídica. Docente e investigadora en el ámbito de la victimización infantojuvenil en línea y la ciberpsicología. Oradora del TEDx-Tarragona 2018 y ponente en numerosos congresos y jornadas. Ha publicado más de 20 artículos y es coautora de varios libros sobre la influencia de las TIC y las redes sociales en el desarrollo y comportamiento de niños, niñas y adolescentes. Coordinadora del primer máster oficial en Ciberdelincuencia de España, en la Universitat Internacional de Catalunya (UIC) y el Centro Terapéutico y Jurídico de la Fundación Vicki Bernadet. Es miembro del Consejo Asesor de la Fundación Barça en su proyecto contra el *bullying*.

El encargo y la creación de este recurso de aprendizaje UOC han sido coordinados por la profesora: Irene Montiel Juan (2020)

Primera edición: febrero 2020

Av. Tibidabo, 39-43, 08035 Barcelona
Realización editorial: FUOC

Índice

Introducción

El ciberespacio constituye un entorno virtual reconocidamente victimogénico (Agustina, 2014; Herrera Moreno, 2006; Miró, 2012) que proporciona características diferenciales tanto al hecho o situación victimizante, como al proceso de victimización y desvictimización.

En este módulo didáctico definiremos en qué consiste la cibervictimización a partir de los aspectos y conceptos victimológicos clave para su comprensión. Se definirá la cibervictimización económica, política y social, y se expondrá la incidencia y la prevalencia en función de fuentes oficiales y encuestas de victimización, además de analizar las posibles causas de la «cifra negra» relacionada con las cibervíctimas.

Objetivos

Los objetivos que deberán alcanzar los estudiantes una vez trabajados los contenidos de este módulo son los siguientes:

1. Comprender en qué consiste la cibervictimización a partir de conceptos relacionados, como la victimología, la victimología del desarrollo, la desvictimización, la victimización secundaria, la revictimización, la polivictimización y la victimización en línea múltiple.

2. Conocer las distintas formas de cibervictimización: económica, social y política.

3. Conocer la incidencia y la prevalencia de la cibervictimización, y comprender el problema de la cifra negra y sus posibles causas.

1. Conceptos y aspectos clave para entender la cibervictimización

Se puede definir la **cibervictimización** como la experiencia de violencia interpersonal en línea. Esto es, un ataque o agresión a través de cualquier medio tecnológico que atenta contra bienes jurídicos protegidos, como el **honor** (por ejemplo, agresiones verbales o psicológicas, etc.), la **libertad sexual** (por ejemplo, la distribución inconsentida de cualquier información íntima o sexual de la víctima), la **libertad** (por ejemplo, el control o vigilancia y las amenazas), la **dignidad** (por ejemplo, ciberodio) o incluso el **patrimonio** (por ejemplo, el fraude). En un sentido más amplio, se incluyen también aquellas situaciones que no están tipificadas expresamente como delito, como el *cyberbullying*, el *online harassment*, la sextorsión, etc., pero son potencialmente dañinas para sus víctimas.

Para comprender el fenómeno de la cibervictimización, debemos tener claros algunos conceptos victimológicos clave.

Finkelhor (2007) describe la **violencia interpersonal o victimización**, como el «daño que se produce en individuos debido a otros actores humanos que se comportan de formas que violan las normas sociales». La victimización o violencia interpersonal difiere de otros acontecimientos vitales negativos o experiencias de violencia no interpersonales, tales como accidentes, enfermedades o desastres naturales.

Tamarit (2006) define la **victimología** como la «ciencia multidisciplinar que se ocupa del conocimiento de los procesos de victimación y desvictimación, es decir, del estudio del modo en que una persona deviene víctima, de las diversas dimensiones de la victimación (primaria, secundaria y terciaria) y de las estrategias de prevención y reducción de la misma, así como del conjunto de respuestas sociales, jurídicas y asistenciales tendentes a la reparación y reintegración social de la víctima».

Por su parte, la perspectiva teórica de la **victimología del desarrollo** (Finkelhor, 2007), defiende que los niños sufren la misma victimización que los adultos, pero, a su vez, se encuentran en una posición de mayor riesgo para la vivencia, directa o indirecta, de otras muchas victimizaciones vinculadas, principalmente, a su nivel de dependencia, lo que nos lleva a considerarlos el grupo de edad más vulnerable en el ámbito victimológico. Además de su posición de dependencia, las víctimas menores suelen caracterizarse por altos o totales

Cibercrímenes sociales

Los menores de edad son el grupo más victimizado por cibercrímenes sociales como el ciberacoso. Los de tipo sexual están estrechamente vinculados con la pornografía infantil o imágenes de abuso sexual infantil.

niveles de inconsciencia respecto a la victimización, lo que las convierte en víctimas ideales (Herrera Moreno, 2006), aspecto que tendrá importantes implicaciones en las consecuencias psicológicas y sociales que puedan derivarse.

La victimización puede ser entendida como hecho (elemento objetivo) y como proceso (elemento subjetivo).

Como **hecho**, se refiere a las distintas formas que puede adoptar (por ejemplo, *cyberbullying*, *online grooming*, ciberodio, ciberfraude, etc.). Como **proceso**, se refiere a la experiencia individual y subjetiva de la víctima de asimilación e interpretación del hecho y aparición de síntomas o daño. Este proceso está mediado por múltiples factores, como su personalidad, su capacidad cognitiva, sus habilidades de resiliencia, la red de apoyo, las características del hecho en sí, del victimario y la relación con este, entre otros elementos.

La **victimización primaria** se refiere al daño producido directamente por el delito o la experiencia. Por otra parte, el impacto derivado de la reacción social y el tratamiento posterior por parte de la policía, el sistema de justicia, los profesionales sanitarios, etc., recibe el nombre de **victimización secundaria**.

Evidencias digitales del abuso

En el caso de la cibervictimización, la difusión de las evidencias digitales del abuso (por ejemplo, insultos, imágenes íntimas o embarazosas, etc.) puede incrementar el sufrimiento de la víctima y dificultar su reajuste psicológico, constituyendo en cierta manera una forma de victimización secundaria.

La **desvictimización** es el proceso inverso a la victimización, de reparación o «reconstrucción», por el que la víctima integra su experiencia y vuelve a construir nuevos objetivos personales y a recuperar el control sobre su propia vida.

> «De lo que se trata, en definitiva, es de que la víctima comience de nuevo a vivir y no meramente se resigne a sobrevivir.»
>
> E. Echeburúa (2004). *Superar un trauma*. Madrid: Pirámide.

También se entiende como el objeto y el fin de la atención integral a la víctima, y como un proceso de carácter intervencionista y preventivo que la hace posible.

La literatura científica ha demostrado ampliamente que, tanto en menores como en adultos, cualquier forma de victimización está íntimamente relacionada con otras, tanto dentro como fuera de la red.

La experiencia de múltiples formas de victimización o violencia interpersonal recibe el nombre de *polivictimización* (Finkelhor, Ormrod, Turner y Hamby, 2005). Hamby y Grych (2013) señalaron que el estudio de la coocurrencia de las diferentes formas de victimización, es decir, concebir que están conectadas entre ellas, constituye un enfoque más coherente de la realidad de las personas.

Polivictimización en menores

En este sentido, Pereda, Abad y Guilera (2015) destacan una importante relación en menores entre la condición de polivíctima y las victimizaciones por parte de cuidadores (físicas y psicológicas), la victimización sexual (especialmente por adultos desconocidos) y la victimización electrónica.

La acumulación de victimizaciones distintas perjudica gravemente el bienestar de las víctimas y su desarrollo psicosocial, en mayor medida que la experimentación de una forma de victimización concreta de manera reiterada (**cronicidad**) e incrementa la probabilidad de volver a ser victimizado en el futuro (**revictimización**). En el ámbito de menores, se ha comprobado que es frecuente la experimentación de distintas formas combinadas o concatenadas de victimización a través de las TIC, lo que se conoce como **victimización en línea múltiple**, (*sexting*, *online grooming*, sextorsión, *cyberbullying*, etc.) (Montiel, Carbonell y Pereda, 2016).

El **ciberespacio** constituye un entorno virtual reconocidamente victimogenésico (Agustina, 2014; Herrera Moreno, 2006; Miró, 2012), que proporciona características diferenciales tanto al hecho o situación victimizante como al proceso de victimización. Las características propias de este contexto virtual (incorporeidad en las relaciones en línea, simultaneidad de las experiencias, ausencia de límites geográficos y políticos, accesibilidad 24/7, velocidad, reducción de inhibiciones y sensación de anonimato y de distancia segura, escala, alcance, etc.) afectan, sin duda alguna, a los procesos de victimización y desvictimización, especialmente en los aspectos siguientes:

- Perfeccionamiento de las estrategias empleadas por el agresor para contactar, perseguir o vigilar a sus víctimas mediante aplicaciones y redes sociales, y posibilidad de adoptar múltiples identidades para hacerlo.

- Incremento de confianza en sí mismo gracias a la elevada probabilidad de éxito y el refuerzo o aprobación social en línea por grupos o foros con los mismos intereses o actitudes.

- Ausencia de percepción de riesgo por el anonimato, la minimización de la autoridad y la ausencia de guardianes eficaces. También las víctimas minimizan los riesgos que asumen por una sensación de distancia segura y de protección ficticia.

- Efecto desinhibitorio que facilita las conductas delictivas a los agresores motivados y elevan las probabilidades de que los usuarios incurran en conductas de riesgo y acaben siendo cibervictimizados (por ejemplo, ingresando material sensible en el ciberespacio, como imágenes íntimas de sexting, interactuar con personas desconocidas en línea o ingresar datos económicos y contraseñas).

- Incremento de víctimas potenciales por la implantación de internet en la vida cotidiana de las personas y las instituciones públicas y privadas, y la posibilidad de atacar simultáneamente a varias víctimas.

- Importancia del papel que juega la víctima en su propia victimización por el ingreso, consciente o inconsciente, de todo tipo de información/material sensible en el ciberespacio, la interacción con potenciales agresores y las estrategias de autoprotección empleadas.

- Mayor velocidad e intensidad a la hora de ganarse la confianza de la víctima y establecer relaciones.

- Inescapabilidad de las víctimas y ausencia de lugares seguros por la accesibilidad 24/7, que aumenta la angustia e indefensión en la víctima.

- Posible publicidad y difusión del ataque, amplificando las consecuencias negativas para la víctima y su entorno.

- Posible cronificación de la victimización, revictimización por el mismo o distintos agresores y polivictimización, lo que incrementa su vulnerabilidad dentro y fuera de la red.

- Dificultades en los procesos de desvictimización por la imposibilidad de retirar o destruir muchas veces las evidencias digitales del abuso y por la pérdida de control sobre los procesos de revelación.

- Minimización del daño o impacto por parte de los profesionales que deben atender a las víctimas por el hecho de tratarse de ataques que no contienen el elemento físico cara a cara.

- Mayor dificultad para asumir la propia victimización, ponerle nombre, liberarse de la culpa y pedir ayuda o denunciar (*naming*, *blaming*, *claiming*).

En definitiva, el ciberespacio constituye un reconocido espacio victimogénico cuya arquitectura digital modifica las dinámicas de victimización y desvictimización, facilitando la acción del ciberagresor motivado, incrementando la vulnerabilidad victimal de aquellos que ingresan material sensible en la red sin las medidas de autoprotección necesarias y dificultando su proceso de desvictimización o reajuste cognitivo y emocional.

1.1. Teoría de las actividades cotidianas

La principal teoría criminológica aplicada al estudio de la ciberdelincuencia y la cibervictimización es la **teoría de las actividades cotidianas (TAC)** (Cohen y Felson, 1979).

Probabilidad de la delincuencia

Para Cohen y Felson, la probabilidad de la delincuencia es una función multiplicativa de la convergencia en el espacio-tiempo de tres elementos: un delincuente motivado para el delito, una víctima apropiada y la ausencia de control social.

Este modelo teórico se relaciona en la actualidad con el énfasis en los factores geográficos o espaciales de la llamada criminología ambiental y tiene su reflejo práctico en la proliferación de mapas sobre lugares de victimización y concentración delictiva.

Miró (2013) plantea una versión adaptada de la TAC original para comprender la ciberdelincuencia. Este autor considera que más que la actuación de guardianes y de gestores del lugar, lo relevante es la propia **actuación de la víctima** en su propia protección («autoprotección»), ya que un objetivo será más adecuado cuanto menos protegido esté. Mientras Felson (1998) entendía que para que un objetivo fuese considerado adecuado debía tener valor desde la perspectiva del delincuente (*value*), inercia, visibilidad física y accesibilidad (VIVA), Miró (2013) considera que en el ciberespacio, la adecuación de un bien u objeto dependerá de que haya sido introducido en internet (lo cual en ocasiones será determinado por las propias acciones de la potencial víctima), de que esté más o menos protegido, y de la interacción del usuario que lo haga accesible y visible a los potenciales agresores motivados. De esta forma, pasamos del acrónimo VIVA al acrónimo ISI: *introduction*, *selfprotection*, *interaction* (introducción, autoprotección e interacción).

2. Fenomenología de la cibervictimización

La mayoría de las tipologías de cibervictimización tienen su origen en la revisión de estudios sobre esta temática, donde se recogen aquellos conceptos que más comúnmente aparecen en la literatura científica o incluso institucional, pero se desconoce su validez empírica. Además, suelen estar diseñadas pensando en los menores de edad como víctimas.

Por ejemplo, EU Kids Online (2008), a partir de la revisión exhaustiva de las investigaciones llevadas a cabo en 21 países europeos desde el año 2006, propone una matriz compleja de riesgos en línea para los menores que tiene en cuenta el papel que adopta el menor (contenido-receptor de contenidos, contacto-participante o conducta-actor) y la naturaleza del riesgo (comercial, agresiva, sexual o ideológica), que da lugar a doce tipos de situaciones de riesgo (Livingstone y Haddon, 2009, p. 10), tal como muestra la tabla 1. Si bien, y aunque no se refiere específicamente a la cibervictimización interpersonal, sino a riesgos en general, podría aplicarse igualmente a víctimas mayores de edad.

Tabla 1. Riesgos relacionados con el uso de los y las menores de internet

	Contenido Receptor de contenidos masivos	**Contacto Participante en una actividad *online* (iniciada por un adulto)**	**Conducta Perpetrador o víctima en un intercambio entre iguales**
Agresividad/Violencia	Contenido violento o agresivo	Acoso	*Bullying*, acoso entre iguales
Sexual	Contenido pornográfico	*Grooming*, abuso sexual o explotación	Acoso sexual, *sexting*
Valores	Contenidos racistas o que inciten al odio	Persuación ideológica	Contenido generado por usuario potencialmente peligroso
Comercial	Marketing encubierto	Uso indebido de los datos personales	Juego, violación de derechos de autor

Fuente: adaptada y traducida por M. Garmendia *et al.* (2011). *Riesgos y seguridad en internet: Los menores españoles en el contexto europeo.* Universidad del País Vasco / Euskal Herriko Unibertsitatea, Bilbao: EU Kids Online, desde www.eukidsonline.net.

La clasificación criminológica más aceptada es la propuesta por Miró (2012), según la cual, en función del móvil o motivación criminal y los bienes atacados, se pueden distinguir tres tipos básicos de cibercrimen: económico, político y social. Estos dan lugar a tres categorías diferenciadas de cibervicictimización.

1) Cibervictimización económica

La cibervictimización económica es la experiencia que se deriva del ataque contra bienes jurídicos patrimoniales u otros como la intimidad o la seguridad de los sistemas, pero siempre con el objetivo de obtener un beneficio económico, y la víctima puede ser una persona o una entidad. Incluye la recepción

de *spam*, infecciones por *malware*, *spyware*, *phishing*, *pharming* o el *hacking* directo, entre otros, como ataques mediales que suelen formar parte de una cadena de ataques que pueden terminar en una defraudación del patrimonio de la víctima o en la utilización de su sistema para la comisión de otro tipo de infracciones que menoscaben su patrimonio. También suelen emplearse técnicas de ingeniería social, mediante las que se manipula o engaña a las personas para que faciliten información o contraseñas que serán usadas para conseguir el fin del delincuente (por ejemplo, en el fraude del CEO).

Algunas de las formas más conocidas de ciberfraude son los cometidos con tarjetas de crédito, cheques, las estafas de inversión, el *auction fraud*, las estafas piramidales realizadas a través de internet, las estafas de la lotería, así como los ataques de *scam*, en los que se prometen cantidades importantes de dinero a cambio de pequeñas transferencias relacionadas con ofertas de trabajo, premios u otros, aunque van transformándose continuamente.

La pornografía infantil puede considerarse tanto una forma de cibervictimización social-sexual como económica, porque internet se utiliza tanto para acceder y acosar a menores y producir este material, como para compartirlo y venderlo en comunidades o redes de personas con intereses pedófilos en común (Beech, Elliott, Birgden y Findlater, 2008).

2) Cibervictimización política

La cibervictimización política se deriva de los cibercrímenes que tienen un objetivo ideológico o institucional e incluyen los delitos de odio, la ciberguerra, el ciberterrorismo y el hacktivismo o ciberativismo político, mediante ataques de denegación de servicios contra páginas web, etc. Estas conductas también pueden ser realizadas por grupos organizados con fines políticos o religiosos que utilizan internet para difundir un determinado mensaje político o como forma de ataque a un estado u organizaciones no gubernamentales (Curran, Concannon y Mckeever, 2008). Las víctimas suelen ser colectivos o estados.

La **guerra cibernética** o **ciberguerra** se define como «las acciones de un estado-nación para penetrar en los ordenadores o redes de otra nación con el fin de causar daños o trastornos».

El **ciberterrorismo** consiste en la utilización de las TIC para la realización de ataques premeditados y políticos contra sistemas de información que son un potencial objetivo, así como la difusión de sus fines y logros, con la consiguiente puesta en peligro de los intereses individuales de las personas y la afectación de la paz social como en cualquier otra forma de amenaza terrorista (Miró, 2012). Esto incluiría comportamientos como difundir el mensaje terrorista mediante páginas web y redes sociales, ayudar a sus actividades por medio de la difusión interna de información (solicitud de financiación, reclutamiento, adoctrinamiento, etc.) o de ataques informáticos directos.

Los **delitos de odio** o *hate speech* no corresponden propiamente a unas categorías jurídicas concretas, sino que se refieren a un conjunto de conductas que, en ocasiones, apuntan a acciones típicas nuevas, y en otras determinan la cualificación de conductas ya tipificadas en el Código penal o en normas administrativas. Requieren que el acto constituya una infracción penal y que sea producto de un prejuicio del autor hacia la víctima por pertenecer a un colectivo vulnerable al odio, normalmente por motivos de raza, religión, ideología, género u orientación sexual. Es decir, la víctima (o el objetivo) se elige intencionadamente por el autor por su pertenencia (real o presunta) a un colectivo al que se desea transmitir rechazo, hostilidad o intimidación.

Miró (2016), explica que existen dos problemáticas distintas en este ámbito:

- Por un lado, internet como foro de radicalización violenta usado, particularmente, aunque no solo, por grupos terroristas yihadistas para el reclutamiento de miembros o para la mera difusión de mensajes de odio o de terror (Cano, 2008; Thompson, 2011). Algunas de las personas reclutadas podrían ser consideradas víctimas de manipulación y abuso psicológico similar al que tiene lugar en las sectas.

- Por otro, la aparición de todo un conjunto de conductas ofensivas y expresiones de comunicación violenta más allá del propio discurso del odio tradicional, particularmente en redes sociales como Facebook y Twitter (Djuric *et al*., 2015).

3) Cibervictimización social

Por último, la cibervictimización social deriva de los cibercrímenes sociales que afectan a bienes jurídicos personalísimos, como la libertad, el honor, la indemnidad o la libertad sexual. Según Montiel, Carbonell y Pereda (2016), se pueden distinguir dos grandes grupos:

- La **victimización sexual en línea**, que incluye situaciones con un marcado componente sexual, como el ciberacoso sexual o sextorsión y el *online grooming* a menores. En un sentido amplio, se puede definir como la experiencia de algún tipo de presión a través de cualquier medio tecnológico para obtener cooperación o contactos sexuales indeseados (por ejemplo, compartir información sexual, enviar imágenes sexuales o realizar alguna conducta sexual en contra de la voluntad de la víctima) y/o la distribución inconsentida de cualquier información íntima o sexual de la víctima (mensajes o imágenes) (Gámez-Guadix, Almendros, Borrajo y Calvete, 2015).

- La **victimización no sexual en línea**, que no contiene necesariamente elementos sexuales, e incluye el *cyberbullying* o ciberacoso entre iguales y el *cyberstalking* o la violencia de pareja en línea. En un sentido amplio, se puede definir como la experiencia a través de cualquier medio tecnológico

de humillaciones, vejaciones, insultos, persecución o control de manera intencionada y reiterada.

3. Incidencia y prevalencia

3.1. Incidencia

Los datos sobre incidencia de la cibervictimización son, en general, escasos, y suelen estar desactualizados y descentralizados, pues provienen de las administraciones públicas, quienes disponen de información limitada, fragmentada y, a veces, poco representativa de la población comunitaria.

Páginas web de interés

- Anuarios y estadísticas. Ministerio del Interior
- Portal estadístico de criminalidad. Ministerio del Interior
- Portal estadístico. Ministerio del Interior

En España, el Sistema Estadístico de Criminalidad (SEC) recoge, desde el año 2007, la información estadística que computa la delincuencia conocida y registrada por las Fuerzas y Cuerpos de Seguridad (Cuerpo Nacional de Policía, Guardia Civil, Policía Foral de Navarra y distintos cuerpos de policía local). Desde el año 2011, también recoge la información estadística sobre ciberdelincuencia siguiendo la clasificación adoptada por el **Convenio sobre cibercriminalidad** o **Convenio de Budapest**.

Sistema Estadístico de Criminalidad (SEC)

La diferencia entre victimización y víctima se puede ejemplificar con el siguiente supuesto: una persona presenta una denuncia y manifiesta que en un determinado período de tiempo, ha sido objeto de tres hechos de malos tratos en el ámbito familiar y un delito de amenazas a través de las TIC. Además, en esta misma denuncia manifiesta que su hijo de tres años también ha sido objeto de malos tratos en una ocasión.

- **Total de denuncias**: 1
- **Total de víctimas**: 2
- **Total victimizaciones**: 5 (3 hechos de malos tratos al denunciante, 1 delito de amenazas al denunciante y 1 hecho de malos tratos al niño)

Según los datos del *VI Informe sobre cibercriminalidad*, en 2018, las victimizaciones registradas por el SEC sumaron un total de 84.607, un 35,5 % más que el año 2017. Entre el año 2014 y el 2018, se observa un crecimiento del 107 % en las cibervictimizaciones registradas (tabla 2), lo que puede indicar un aumento real de las víctimas o un aumento de los hechos denunciados, influenciado por las reformas penales implementadas en este período.

Tabla 2. Evolución de las victimizaciones* registradas en España entre 2014 y 2018 según edad

Grupo de edad	2014	2015	2016	2017	2018	2014-2018
Adultos	38.811	44.703	51.768	59.974	82.138	**111,64 %**
Menores	1.833	2.004	2.110	2.287	2.319	**26,51 %**
Edad desconocida	146	153	568	158	150	**2,74 %**

* El término *victimización* se refiere al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal, y no a personas individuales.

Fuente: elaboración propia a partir de los datos de los Informes sobre cibercriminalidad.

Grupo de edad	2014	2015	2016	2017	2018	2014-2018
Total	40.790	46.860	54.446	62.419	84.607	**107 %**

* El término *victimización* se refiere al número de hechos denunciados por personas en los cuales manifiestan ser víctimas o perjudicados por alguna infracción penal, y no a personas individuales.

Fuente: elaboración propia a partir de los datos de los Informes sobre cibercriminalidad.

El fraude informático es la tipología delictiva con mayor incidencia en todos los grupos de edad establecidos (a excepción de los menores de edad), y de manera especial en los rangos de edad que va de los veintiséis años en adelante, seguida de las amenazas y coacciones. Las víctimas menores de edad son más vulnerables a otro tipo de hechos delictivos, en concreto a las amenazas y coacciones (40 %) y los delitos sexuales (31 %) (tabla 3).

Tabla 3. Victimizaciones registradas según grupo penal y edad (2018)

	Menores de edad	De 18 a 25 años	De 26 a 40 años	De 41 a 50 años	De 51 a 65 años	Mayores de 65 años	Edad desconocida	Total edad
Acceso e interceptación ilícita	258	480	831	539	368	57	7	2.540
Amenazas y coacciones	851	2.003	4.555	2.824	1.780	394	51	12.458
Contra el honor	102	190	502	355	258	49	36	1.492
Contra la propiedad industrial/intelectual	0	2	8	14	12	17	1	54
Delitos sexuales	818	44	31	23	11	3	6	936
Falsificación informática	93	328	772	498	347	120	3	2.161
Fraude informático	185	8.407	22.776	16.389	13.035	3.310	46	64.148
Interferencia en los datos y en el sistema	12	57	215	265	227	42	0	818
Total grupo penal	**2.319**	**11.511**	**29.690**	**20.907**	**16.038**	**3.992**	**150**	**84.607**

Fuente: Ministerio del Interior, *V Informe sobre cibercriminalidad* (2017).

La mayoría de las víctimas de ciberdelincuencia pertenecen al sexo masculino (54,5 %), tienen entre veintiséis a cuarenta años y son objeto, principalmente, de los delitos de fraudes informáticos, amenazas y coacciones, y acceso e interceptación ilícita. Sin embargo, si se analiza la distribución global de incidentes conocidos por ámbito y sexo, las mujeres exceden en porcentaje a las víctimas de sexo masculino cuando se trata de hechos relacionados con el acceso e interceptación ilícita, contra el honor, los delitos sexuales y la falsificación informática (tabla 4).

Tabla 4. Victimizaciones registradas según grupo penal y sexo (2018)

	Masculino	Femenino	Se desconoce	Total sexos
Acceso e interceptación ilícita	1.019	1.519	2	2.540
Amenazas y coacciones	6.454	5.972	32	12.458
Contra el honor	680	799	13	1.492
Contra la propiedad industrial/intelectual	37	17	0	54
Delitos sexuales	267	663	6	936
Falsificación informática	1.049	1.110	2	2.161
Fraude informático	34.159	29.954	35	64.148
Interferencia en los datos y en el sistema	510	307	1	818
Total grupo penal	**44.175**	**40.341**	**91**	**84.607**

Fuente: Ministerio del Interior, *VI Informe sobre cibercriminalidad* (2018).

Por otro lado, el Ministerio del Interior informa de que los delitos de odio registrados en el año 2017 aumentaron un 11,6 % respecto al 2016 (1.419 casos). Los ámbitos que han registrado un mayor número de incidentes son los de racismo y xenofobia (37 %), ideología (31 %) y orientación o identidad sexual (19 %). Las injurias, hechos discriminatorios y amenazas se computan como los hechos delictivos que más se repiten, donde internet (36,5 %) y las redes sociales (17,9 %) son los medios más empleados para la comisión de estos hechos, aunque también se emplean otras vías de comunicación, como la telefonía/comunicaciones (15,4 %) y los medios de comunicación social (13,5 %).

Lecturas complementarias

Instituto Nacional de Ciberseguridad (2017). En España se gestionan diariamente cerca de 400 incidentes de ciberseguridad [en línea].

Centro criptológico nacional (2019). Informes CCN-CERT Públicos [en línea].

Durante el año 2018, el Centro de Respuesta a Incidentes de Seguridad e Industria (CERTSI), operado de forma coordinada por el Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC), ha gestionado en España 111.519 incidentes de ciberseguridad. De ellos, 102.414 afectaban a ciudadanos, empresas y la red académica y 722 a operadores críticos, que son las empresas que gestionan infraestructuras esenciales para el funcionamiento correcto de cada sector económico de un país (por ejemplo, financiero, energético o transportes), lo cual podría estar relacionado con el ciberespionaje y el ciberterrorismo, pero no se dispone de datos al respecto.

3.2. Prevalencia

En una revisión de estudios realizada por Berhg y Junger (2018), se incluyeron nueve encuestas de victimización realizadas en Europa con muestras representativas de la población general (la edad mínima fue de doce años en algunos

países y catorce en otros). Las tasas anuales de prevalencia de la cibervictimización oscilan entre el 2 % y el 15 % para el *malware*, entre el 1 % y el 6 % para el *hacking*, entre el 1 % y el 3 % para el fraude en las compras en línea, entre el 1 % y el 2 % para el fraude bancario, menos del 1 % para otros tipos de fraude y un máximo del 3 % para algún tipo de acoso en línea como el ciberacoso (1 %) o amenazas en línea (1 %). Sin embargo, no se puede estimar hasta qué punto las diferencias encontradas entre estudios pueden deberse a aspectos metodológicos, a diferencias reales entre países o a variaciones a lo largo del tiempo.

Según la *Encuesta mundial sobre fraude y delito económico*, que elabora la empresa de consultoría PwC cada dos años a partir de la opinión de más de siete mil compañías de todo el mundo, en 2018, el 49 % de las empresas de todo el mundo han sido víctima de algún delito económico en los últimos dos años (frente al 30 % en 2009). En España, este porcentaje es del 54 % (frente al 35 % en 2009), en el Reino Unido y Alemania el 50 %, y en Estados Unidos el 53 %.

Sin embargo, a nivel individual, el Eurobarómetro 2018 recoge que no más del 20 % de los encuestados (28.093) han sido víctimas de fraude en línea, excepto Chipre (23 %) y el Reino Unido (22 %). En España, tan solo un 6 % lo ha sufrido. La media en los veintiocho países de la Unión Europea es del 16 %. El grupo de edad más victimizado es el formado por jóvenes entre quince y veinticuatro años (18 %), y el que menos, el formado por los mayores de cincuenta y cinco años (9 %).

En España, el Centro Crímina para el estudio y prevención de la delincuencia, de la Universidad Miguel Hernández de Elche, ha llevado a cabo dos estudios destacables en este ámbito, uno con menores y otro con adultos.

En uno de ellos participaron 2.038 menores de la provincia de Alicante entre doce y dieciocho años, con el objetivo de determinar la prevalencia de la cibervictimización económica y social en la población adolescente. Los resultados muestran que el 78,9 % de los estudiantes han sufrido algún tipo de ciberataque económico y el 53,7 % algún tipo de cibercrimen social, y además el acoso no sexual es más frecuente que el de tipo sexual (50,6 % frente a 5,7 %).

Dentro de los ciberdelitos económicos, se incluyen los llamados *ataques mediales*, aquellos que son los previos para cometer ataques económicos finales, como el envío de *spam* o la infección por *malware* (17 % y 72 %, respectivamente), y los finales como el fraude (3,4 %). Los cibercrímenes sociales hacen referencia al acoso (amenazas, coacciones, colgar información personal con acusaciones falsas, etc.) y al acoso sexual, donde destacan los mensajes sexuales reiterados a través de internet o del móvil.

También sobre cibervictimización en adolescentes españoles, destaca el estudio de Montiel, Carbonell y Pereda (2016), en el que participaron 3.897 estudiantes de educación secundaria de entre doce y diecisiete años. Un 61 % re-

portó haber sufrido algún tipo de victimización electrónica durante el último año, un 39,5 % por cibervictimización sexual y un 53,4 % por cibervictimización no sexual. Un 35 % de los adolescentes experimentaron victimización en línea múltiple y la mayoría de ellos (88 %) vivieron tanto cibervictimización sexual como no sexual. Entre las cibervíctimas, predominaban las experiencias de ciberacoso (81 %), de exposición indeseada a contenido sexual (39 %), *online grooming* por un adulto (27 %) y violación de la intimidad (23 %), pero también en menor medida habían experimentado *happy slapping* (3 %), coacción y presión sexual (10 % y 19 %, respectivamente).

En el otro estudio realizado por Crímina, participaron 500 españoles usuarios de internet entre dieciocho y sesenta y cinco años, con el objetivo de determinar la prevalencia de la cibervictimización económica y social en la población adulta. Los resultados del estudio muestran que el 87,2 % de los sujetos de la muestra ha sufrido al menos alguna de las formas de cibervictimización medidas, el 86,6 % de tipo económico y el 21,6 % de tipo social (frente al 78,9 % y el 53,7 %, respectivamente, en la muestra de menores). El 43 % ha recibido *spam*, el 75 % infección por *malware* y el 6,6 % se declara víctima de fraude.

Los cibercrímenes sociales presentan una menor prevalencia que el cibercrimen económico, especialmente el acoso de tipo sexual (2,2 %), igual que ocurría en la muestra de menores. Se encontró que en los adultos la prevalencia de ciberacoso sexual es mucho más baja que en menores (2,2 % frente a 5,7 %). Entre las conductas de ciberacoso sexual, la que más se produce es el envío de mensajes con contenido de carácter sexual (1,2 %), seguido, con el mismo porcentaje, de haberse visto obligado en al menos una ocasión a realizar comportamiento de tipo sexual a través de la webcam o haberse visto obligado a enviar fotografías con contenido sexual (0,2 %).

En un estudio realizado por la Universitat Oberta de Catalunya en el que participaron 753 estudiantes universitarios mayores de 18 años, se obtuvo una prevalencia general de cibervictimización del 67 %. Como resultado de un análisis de clases latentes, se diferenciaron dos perfiles de cibervíctimas: las que habían sufrido principalmente cibercrímenes económicos constituían el 57 % y las que habían padecido principalmente cibercrímenes sociales el 17 % (Montiel, Tamarit y Malpica, en prensa).

Hasta el momento ha habido muy pocos estudios rigurosos sobre cibervictimización entre la población general, pues la mayoría se han servido de muestras de conveniencia y limitadas a pequeños rangos de edad. Sin embargo, la prevalencia y su tendencia solo puede medirse bien si las muestras son probabilísticas y representativas de la población (adultos y menores) y si se recogen los datos de manera sistemática y periódica. En el futuro, es aconsejable desarrollar algunas categorías principales más abstractas o genéricas que sean de validez duradera, pero que permitan actualizaciones. También deberían estandarizarse los instrumentos de medida y establecerse una clasificación uniforme de las diferentes formas de cibervictimización, así como incorporar en

las encuestas preguntas sobre el impacto o daño a las víctimas y la experiencia de la denuncia o la atención recibida. De esta forma, además de conocer la magnitud de los fenómenos y su evolución temporal, se podría evaluar la eficacia de las medidas que se adoptan para su prevención y tratamiento.

Tanto en los datos de incidencia como de prevalencia, se observa que la cibervictimización económica es más frecuente que la social, o al menos se revela y/o denuncia más, igual que sucede en la delincuencia tradicional. También se observa que los menores de edad son el grupo de edad más victimizado por ciberdelitos sociales de tipo sexual, mientras en adultos es más frecuente la cibervictimización económica.

3.3. Cifra negra

Las estadísticas oficiales disponibles sobre ciberdelincuencia y cibervictimización subestiman las dimensiones reales del problema porque los porcentajes no se corresponden, en ningún caso, con aquellos encontrados a partir de las propias revelaciones de las víctimas mediante encuestas de victimización, sino que reflejan únicamente el volumen de hechos que llegan a conocimiento de las autoridades policiales y/o judiciales, ignorando la llamada «**cifra negra**» de la ciberdelincuencia.

Según Kshetri (2010), las características de los cibercriminales, las cibervíctimas y las agencias policiales se refuerzan entre ellas dando lugar al «**círculo vicioso del cibercrimen**». La lentitud de los avances legales, la heterogeneidad de las leyes anticibercrimen, la falta de recursos y la inexperiencia de los cuerpos policiales implicados en complejas investigaciones tecnológicas que no siempre llegan a ser resueltas actúan como factores facilitadores de las conductas ilícitas de los cada vez más experimentados y hábiles cibercriminales, que ven reforzada su confianza y expectativas de éxito e impunidad.

Se pueden identificar tres motivos básicos que podrían explicar la enorme cifra negra de la cibervictimización:

1) Dificultades en el registro de la información estadística sobre cibervictimización.

2) Dificultades para el procesamiento, especialmente debido a la dificultad para determinar los autores (por el anonimato en la red, la falta de colaboración de la empresa de servicios, la determinación del sistema informático desde el que se ha realizado la acción, la transnacionalidad del delito, etc.).

3) Falta de denuncia por parte de la víctima (porque se desconoce la existencia de un delito, se conoce pero no se acepta la condición de víctima o no se quiere evidenciar, por miedo a la venganza, por vergüenza o culpa, o por falta de confianza en las fuerzas y cuerpos de seguridad o el sistema de justicia penal).

Las cibervíctimas, y especialmente los menores, presentan pobres mecanismos de defensa y suelen acceder a las demandas del cibercriminal, poseen una baja o inexistente confianza en las agencias y fuerzas legales y, en consecuencia, la tasa de denuncias es muy baja y la cifra negra muy elevada, lo que refuerza todavía más la conducta de los cibercriminales.

Comprender y aceptar la propia victimización y la gravedad de los hechos, asumir la condición de víctima, reconocer la necesidad de ayuda y, además, sentirse merecedor de la misma, solicitarla, liberado de los sentimientos de vergüenza y culpa, junto a la posibilidad de tener que afrontar una intervención psicológica, policial y/o judicial poco especializada, o la creencia de que «nada cambiará», son aspectos complejos que se suman al propio impacto psíquico derivado de la experiencia de la cibervictimización y alejan a la víctima de la idea de la denuncia.

En el caso de la cibervictimización económica y política, muchas empresas y gobiernos prefieren no desvelar su situación para proteger su imagen y no poner en evidencia la vulnerabilidad de sus sistemas.

Delitos de odio

En los delitos de odio, por ejemplo, los estudios demuestran que las víctimas son propensas al aislamiento, a la pérdida de fe y de la identidad, a la autoculpa, a la frustración y a la revictimización por deficiencias en las conductas de afrontamiento, por lo que decidir si deben denunciar o no se vuelve una tarea realmente difícil (Kercher, Nolasco y Wu, 2008).

Bibliografía

Agustina, J. R. (2014). «Criminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización». *Cuadernos de política criminal* (vol. 114, n.º 3, págs. 143-178).

Beech, A. R. *et al.* (2008). «The internet and child sexual offending: A criminal review». *Aggression and Violent Behavior* (vol. 13, n.º 3, págs. 216-228).

Bergh, C. M.; Junger, M. (2018). «Victims of cybercrime in Europe: a review of victim surveys». *Crime Science* (n.º 7, págs. 1-15).

Cano Paños, M. A. (2008, diciembre). «Internet y terrorismo islamista: aspectos criminológicos y legales». *Eguzkilore* (n.º 22). San Sebastián.

Cohen, L. E.; Felson, M. (1979). «Social Change and Crime Rate Trends: A Routine Activity Approach». *American Sociological Review* (n.º 44, págs. 588-608).

Curran, K.; Concannon, K.; Mckeever, S. (2008). «Cyber terrorism attacks». En: L. J. Janczewski, A. M. Colarik (Eds.). *Cyber Warfare and Cyber Terrorism*. Hershey-Londres: IGI Global.

Djuric, N. *et al.* (2015). «Hate speech detection with comment embeddings». *Proceedings of the 24th International Conference on World Wide Web Companion*.

Echeburúa, E. (2004). *Superar un trauma*. Madrid: Pirámide.

Finkelhor, D. (2007). «Developmental victimology: The comprehensive study of childhood victimization». En: R. C. Davis, A. J. Lurigio, S. Herman (Eds.). *Victims of crime* (3.ª ed., págs. 9-34). Thousand Oaks, CA: Sage Publications.

Finkelhor, D. *et al.* (2005a). «Measuring poly-victimization using the Juvenile Victimization Questionnaire». *Child Abuse & Neglect* (vol. 29, núm. 11, págs. 1297-1312).

Gámez-Guadix, M. *et al.* (2015). «Prevalence and Association of Sexting and Online Sexual Victimization Among Spanish Adults». *Sexuality Research and Social Policy* (vol. 12, n.º 2, págs. 145-154).

Garmendia, M. *et al.* (2011). *Riesgos y seguridad en internet: Los menores españoles en el contexto europeo* [en línea]. Universidad del País Vasco / Euskal Herriko Unibertsitatea, Bilbao: EU Kids Online. Disponible en: www.eukidsonline.net.

Hamby, S. L.; Grych, J. (2013). *The web of violence: Exploring connections among different forms of interpersonal violence and abuse*. New York: Springer.

Herrera Moreno, M. (2006). «Victimización: aspectos generales». En: E. Baca, E. Echeburúa, J. M. Tamarit (Coords.). *Manual de victimología* (págs. 79-128). Valencia: Tirant lo Blanch.

Kshetri, N. (2010). «Simple Economics of Cybercrime and the Vicious Circle». *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (págs. 38-39 y 42).

Kercher, G.; Nolasco, C.; Wu, L. (2008). *«Hate Crimes»*. Texas: The Crime Victims' Institute Sam Houston State University Criminal Justice Centre Huntsville.

Livingstone, S.; Haddon, L. (2009). *EU Kids Online: Final report* [en línea]. London: LSE, EU Kids Online. Disponible en: eprints.lse.ac.uk/24372/.

Ministerio del Interior (2014, 2015, 2016, 2017, 2018). *Informe de cibercriminalidad* [en línea]. Madrid: Gobierno de España, Ministerio del Interior, Gabinete de Coordinación y Estudios, Secretaría de Estado de Seguridad. Disponible en: www.interior.gob.es/documents/10180/8859844/Informe+2017+sobre+Cibercriminalidad+en+Espa%C3%B1a.pdf/a9f61ddb-3fcf-4722-b9d8-802a424a1a70.

Miró, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*. Madrid: Marcial Pons.

Miró, F. (2013). «La victimización por cibercriminalidad social. Un estudio a partir de la teoría de las actividades cotidianas en el ciberespacio». *Revista Española de Investigación Criminológica: REIC* (n.º 11, art. 5).

Miró, F. (2016). «Taxonomía de la comunicación violenta y el discurso del odio en internet». *IDP. Revista de Internet, Derecho y Política* (monográfico «Ciberdelincuencia y cibervictimización») (n.º 22, págs. 93-118).

Montiel, I. (2016). «Cibercriminalidad social juvenil: La cifra negra. 016). Taxonomía de la comunicación violenta y el discurso del odio en internet». *IDP. Revista de Internet, Derecho y Política* (monográfico «Ciberdelincuencia y cibervictimización») (n.º 22, págs. 119-131).

Montiel, I.; Carbonell, E.; Pereda, N. (2016). «Multiple online victimization of Spanish adolescents: Results from a community sample». *Child Abuse & Neglect* (n.º 52, págs. 124-127).

Pereda, N.; Abad, J.; Guilera, G. (2015). «Victimization and polyvictimization of Spanish youth involved in juvenile justice». *Journal of Interpersonal Violence* (págs. 1-29).

Tamarit Sumalla, J. M. (2006). «La victimología: cuestiones conceptuales o metodológicas». En: E. Baca, E. Echeburúa, J. M. Tamarit (Coords.). *Manual de victimología*. Valencia: Tirant lo Blanch.

Thompson, R. (2011). «Radicalization and the use of social media». *Journal of Strategic Security* (vol. 4, n.º 4).