Cibercriminología y victimización *online*

Colección:
Criminología - Manuales

Coordinadores:
Cristina Rechea Alberola
Antonio Andrés Pueyo
Andrea Giménez-Salinas Framis

Cibercriminología y victimización *online*

José R. Agustina
Irene Montiel Juan
Manuel Gámez-Guadix

EDITORIAL SINTESIS

Consulte nuestra página web: **www.sintesis.com**
En ella encontrará el catálogo completo y comentado

© EDITORIAL SÍNTESIS, S. A.
Vallehermoso, 34. 28015 Madrid
Teléfono: 91 593 20 98
www.sintesis.com

ISBN: 978-84-9171-454-5
Depósito Legal: M-1.633-2020

Impreso en España - Printed in Spain

Índice

Parte III
Tipologías delictivas en cibercriminalidad instrumental, económica y política y delitos del futuro

2

Cyberbullying, cyberstalking *y discurso de odio*

Las TIC constituyen fundamentalmente un contexto social. Este espacio interpersonal fomenta la participación *online* de personas muy diversas a través de foros, chats, redes sociales o aplicaciones como Twitter, Instagram o Facebook. Además, internet se ha convertido en un espacio prominente de socialización, principalmente entre adolescentes y jóvenes. Este medio permite establecer relaciones íntimas con otros y puede favorecer el desarrollo de competencias interpersonales, como la empatía, la gestión de emociones y las habilidades sociales *online*.

De manera paralela, la generalización de internet como medio social también ha dado lugar a diferentes formas de agresión y acoso interpersonal. Así, cabe identificar varios tipos de agresiones electrónicas o cibernéticas que incluyen el acoso moral o laboral, el discurso de odio, la denigración (humillaciones de diversa naturaleza), la revelación de secretos, la suplantación o robo de identidad *(identity theft),* la exclusión o marginación de alguien, la creación de perfiles falsos con ánimo de perjudicar a alguien y la distribución de material personal contra la voluntad de alguien. Las diversas formas de ataque contra la integridad moral, la fama, la intimidad y la libertad, entre otros bienes de la persona que pueden verse afectados, pueden ocasionar un gran malestar y sufrimiento en sus víctimas.

Este capítulo revisa la conceptualización, la fenomenología y las características definitorias de las diferentes manifestaciones de acoso que tienen lugar a través de medios electrónicos. A continuación, se exponen las principales teorías criminológicas y psicológicas que permiten dar cuenta de este fenómeno. Asimismo, se resumen los datos sobre la prevalencia, los factores de riesgo y los perfiles de agresores y víctimas. Por último, se abordan las cuestiones de prevención y tratamiento de las diversas formas de acoso *online* para terminar exponiendo las aproximaciones jurídica y forense ante estas problemáticas.

2.1. Conceptualización y fenomenología de las distintas formas de acosar, insultar y amenazar en el ciberespacio

Los términos *cyberbullying, victimización cibernética, acoso online* o *ciberacoso* se han empleado con frecuencia para hacer referencia a las agresiones repetidas a través de las TIC (Kowalski, Giumetti, Schroeder y Lattanner, 2014; Livingstone y Smith, 2014). Aunque existen algunos matices entre estas denominaciones en función de los estudios y las aproximaciones teóricas, en el presente capítulo emplearemos el término *ciberacoso* como denominación genérica e inclusiva para hacer referencia a las diversas formas de agresión y victimización repetida en el tiempo que se produce a través de medios electrónicos, principalmente internet y el teléfono móvil.

La mayoría de las caracterizaciones sobre ciberacoso disponibles en la literatura científica emplean elementos similares a los considerados para describir el acoso tradicional *offline:* la intención de dañar, la repetición y el desequilibrio de poder (Smith, 2012).

El ciberacoso es intencional. Para considerarlo como tal, el acoso debe ser deliberado y no accidental, y debe ocasionar un daño a alguien. Los actos accidentales (por ejemplo, la difusión inintencionada de una información en un grupo de WhatsApp) no constituyen ciberacoso *per se,* a no ser que, con posterioridad, esa información se utilice para provocar daño a alguien o se distribuya deliberadamente.

El ciberacoso es, por definición, recurrente. Una conducta aislada puede ser considerada como "agresión", pero no constituye acoso. En el caso del ciberacoso, la agresión debe ser repetitiva y prolongarse a lo largo del tiempo. No obstante, es importante señalar que, en el contexto digital, un solo acto iniciado por un único perpetrador puede convertirse en repetitivo por medio de que otros lo compartan, retuiteen o comenten y, por ende, en estos casos cabría calificarlo de acoso.

Un elemento adicional en algunas definiciones de ciberacoso es la diferencia de poder o asimetría entre el agresor y la víctima (por ejemplo, Smith *et al.,* 2008). Este es un criterio frecuente en las conceptualizaciones de acoso tradicional para indicar que el hostigamiento se dirige hacia una víctima que no puede defenderse fácilmente por sí misma.

Sin embargo, este criterio ha sido cuestionado en el caso del ciberacoso. Por ejemplo, en el *cyberbullying* (término habitualmente empleado para referirse al ciberacoso entre menores de edad) se ha señalado que podría *no* ser necesaria una diferencia de poder real entre el agresor y la víctima; el agresor puede ser alguien que simplemente no se atreve a llevar a cabo la agresión cara a cara, pero puede hacerlo *online* amparado por el anonimato. Incluso en estos casos, se ha indicado que en el ciberespacio se producen otras formas de asimetría y desequilibrio de poder, tales como el anonimato o la mayor pericia tecnológica.

En todo caso, es preciso aclarar que el ciberacoso puede ser llevado a cabo por una persona o por un grupo. La naturaleza colaborativa de internet facilita que muchas personas desconocidas entre sí puedan contribuir a perpetrar y mantener el acoso de manera

relativamente sencilla. Por ejemplo, los usuarios de internet pueden compartir rumores perjudiciales o fotos comprometidas de alguien. Además, los colaboradores (personas que no inician la agresión, pero refuerzan al agresor) o los espectadores o *bystanders* (no agreden y no refuerzan, pero tampoco intervienen para evitarlo) pueden contribuir a mantener la situación de ciberacoso.

2.1.1. Diferencias entre el acoso tradicional y el ciberacoso

Algunos investigadores sostienen que el ciberacoso es una extensión del acoso tradicional y, por tanto, es posible extrapolar la evidencia empírica acumulada sobre el acoso tradicional al ciberacoso (Kowalski y Limber, 2007). Otros sugieren que, aunque presentan ciertas características en común, el ciberacoso y el acoso tradicional son dos tipos de acoso únicos. Las actuales perspectivas sobre la relación entre acoso tradicional y ciberacoso se resumen en tres:

1. El ciberacoso puede ser simplemente una forma más para intimidar a otras personas dentro del conjunto de formas posibles del acoso *offline* y *online,* que guardan entre sí una estrecha relación.
2. El acoso cibernético puede proporcionar un mecanismo para decir y hacer cosas a otros que uno nunca diría o haría en interacciones cara a cara: en ese sentido uno podría sustituir al otro.
3. El ciberacoso es un medio de venganza por ser acosado *offline,* por lo que el primero sería la consecuencia del segundo.

Lo que, en todo caso, se desprende de estas tres perspectivas es que acoso *offline* y ciberacoso no son fenómenos independientes, sino más bien parecen estar relacionados de una manera u otra. Aunque existen múltiples similitudes entre el acoso tradicional y el ciberacoso (por ejemplo, intencionalidad y recurrencia), este último presenta algunas características distintivas importantes que se describen a continuación (Smith, 2012).

El ciberacoso depende de cierto grado de experiencia tecnológica. Aunque algunas formas de ciberacoso son más simples (por ejemplo: enviar un mensaje insultante o amenazante), los ataques más sofisticados (como el hackeo de un dispositivo para obtener información personal) requieren una mayor habilidad.

A diferencia del acoso tradicional, el ciberacoso es principalmente indirecto más que cara a cara. Esta característica favorece la "invisibilidad" de los agresores respecto a las reacciones de su víctima al acoso. Así, el agresor generalmente no ve la reacción de la víctima, al menos a corto plazo. Este hecho puede facilitar los mecanismos de desconexión moral respecto a la situación de la víctima, dificultando los sentimientos de empatía y remordimiento en el agresor.

En el caso del ciberacoso, existe una mayor variedad de roles de espectadores u observadores. Cabe identificar tres roles principales de observador en lugar de uno:

1. El observador que está con el perpetrador cuando se envía o publica un acto.
2. El observador que se encuentra con la víctima cuando se produce el acoso.
3. El observador que no está con ninguno de los dos, pero recibe el mensaje o visita el sitio de internet correspondiente en el se ha publicado el acoso.

Cada uno de ellos puede jugar un papel diferente y relevante en la perpetuación de la situación de ciberacoso, lo que debe ser tenido en cuenta en la intervención sobre el mismo.

Un motivo común en el acoso tradicional es la demostración de poder y estatus del agresor frente a los espectadores y la víctima. Este elemento es menos frecuente en el caso del ciberacoso, debido al anonimato percibido en el ciberespacio, aunque igualmente podría estar presente.

Internet aumenta la amplitud de la potencial difusión del ciberacoso. La difusión del ciberacoso puede alcanzar a un gran número de personas en comparación con grupos mucho más reducidos que son la audiencia habitual en el acoso tradicional. Por ejemplo, cuando se publican comentarios denigrantes sobre alguien en un sitio web, el número de personas que puede llegar a leer estos comentarios es potencialmente mucho mayor que en el acoso tradicional.

Finalmente, resulta difícil escapar del acoso cibernético, a diferencia de las formas tradicionales de acoso, en las que una vez que la víctima llega a casa no está expuesta a la situación de acoso laboral o escolar hasta el día siguiente. Cuando se produce ciberacoso, la víctima puede continuar recibiendo mensajes de texto o correos electrónicos, o ver las publicaciones humillantes en internet, donde quiera que se encuentre.

2.2. Definición de términos en la literatura especializada

Partiendo del ciberacoso como concepto inclusivo de las diversas formas de ataque contra la integridad moral, la fama, la intimidad y la libertad de una persona en el ciberespacio, entramos a repasar algunas formas de particulares que se han venido distinguiendo en la literatura especializada en la materia. Obsérvese que se ha excluido el ciberacoso de naturaleza sexual que, por su especificidad, se estudia de forma separada (capítulo 3).

El término *cyberbullying* ha sido empleado con frecuencia para referirse a la agresión entre iguales, normalmente adolescentes o jóvenes (Kowalski *et al.,* 2014). Aunque es menos frecuente, se ha empleado también la denominación de *cyberbullying* para referirse a la agresión entre adultos e, incluso, al acoso que tiene lugar en el contexto laboral o de pareja (por ejemplo, Mowry y Giumetti, 2019).

Smith *et al.* (2008: 376) lo caracterizan como "un acto agresivo e intencional llevado a cabo por un grupo o individuo, usando formas electrónicas de contacto, repetidamente o a lo largo del tiempo sobre una víctima que no puede defenderse fácilmente por sí misma" . De forma más general, Slonje y Smith (2008: 147) lo definen como "una agresión que ocurre a través de los actuales dispositivos tecnológicos y específicamente, los teléfonos móviles o internet". De manera similar, Patchin e Hinduja (2006) lo describen como un daño deliberado y repetido infligido a través de medios electrónicos. Por su parte, Juvonen y Gross (2008) se refieren al *cyberbullying* como el uso de internet u otros dispositivos digitales de comunicación para insultar o amenazar a alguien. Asimismo, Tokunaga (2010: 278) lo define como "cualquier comportamiento realizado a través de medios electrónicos o digitales por individuos o grupos que envían repetidamente mensajes hostiles o agresivos destinados a infligir daño o incomodidad a otros" . A esta definición añade la siguiente aclaración: "En las experiencias de cyberbullying, la identidad del acosador puede o no ser conocida. El acoso cibernético puede ocurrir a través de la comunicación mediante medios electrónicos en la escuela; sin embargo, los comportamientos de cyberbullying también ocurren comúnmente fuera de la escuela".

De una forma más integradora, Willard (2005) identifica siete formas de *cyberbullying:*

- *Flaming*. Consiste en enviar mensajes groseros y vulgares o que muestran enfado sobre alguien a un grupo *online*. Un ejemplo de *flaming* es el envío de un mensaje incendiario a un foro o lista de correo con el objetivo de provocar reacciones de ira en sus participantes.
- *Online harassment*. Supone el envío repetidamente de mensajes ofensivos por correo electrónico o mensajes de texto a una persona.
- *Cyberstalking*. Es el acoso en línea que incluye amenazas de daño o es excesivamente intimidatorio.
- Denigración (humillaciones). Se refiere al envío de mensajes dañinos, falsos o crueles sobre alguien a otras personas, o la publicación de dicho material *online*.
- Mascarada *(masquerade)*. Es una forma de acoso en la que se simula ser otra persona para enviar material que humille o haga quedar mal a alguien.
- *Outing*. Es el envío o publicación de material sobre una persona que contiene información confidencial, privada o vergonzosa, incluido el reenvío de mensajes o imágenes privadas.
- Exclusión. Consiste en excluir cruelmente a alguien de un grupo *online*.

Aunque a veces se han incluido como una forma de *cyberbullying,* los términos *online harassment* o *internet harassment* también han sido empleados de manera independiente para referirse a conductas aisladas (no repetitivas) de acoso en la red. Por ejemplo, Jones, Mitchell y Finkelhor (2012) describen el *online harassment* como las amenazas u otros comportamientos ofensivos entre jóvenes enviados o colgados *online*

para que otros los vean. De forma más genérica, Ybarra, Mitchell, Wolak y Finkelhor (2006) definen el *internet harassment* como un acto público e intencional de agresión hacia otra persona en el contexto digital. En ese mismo sentido, Miró (2013b) entiende que el concepto de *online harassment* debe emplearse para referirse a actos concretos, y no continuados, de *bullying* o *stalking* en el ciberespacio. Por tanto, según Miró incluiría todas las conductas de *cyberbullying* (entre menores) o de *cyberstalking* (cuando se realiza sobre un adulto), siempre que no sean realizadas de forma continuada por el mismo sujeto o sujetos sobre la misma víctima. Las conductas más prototípicas de *online harassment* serían: el envío de mensajes amenazantes o abusivos a través del correo electrónico, la mensajería instantánea o el chat; la publicación de información falsa sobre la víctima; la suplantación de identidad con fin de burla, de obtener información o de dañar de cualquier modo al sujeto; la intimidación o la coacción a través de comunicación escrita o verbal por medio de internet; el insulto o calumnia leve y grave; la incitación a otras personas al acoso, a proferir amenazas o a agredir a la víctima; el envío de *software* malicioso o de material pornográfico u ofensivo para dañar a la víctima, etc. (Miró, 2013b).

Cabe señalar, en todo caso, que con frecuencia los términos *cyberbullying* y *online harassment* han sido empleados en la literatura especializada de forma intercambiable.

Otro término empleado con frecuencia para referirse a formas de ciberacoso es el de cyberstalking. Aunque su traducción al castellano es, literalmente, 'ciberacoso', el *cyberstalking* conlleva una fuerte connotación de hostigamiento, vigilancia y persecución de un individuo contra otro. A menudo, es un término empleado en contextos legales. Por ejemplo, el Departamento de Justicia de EE. UU. define *cyberstalking* como el uso de internet, correo electrónico u otros dispositivos de comunicaciones electrónicas para acosar a otra persona (Reno, 1999). En términos generales, la mayoría de las leyes de *cyberstalking* implican amenazas directas o indirectas contra la víctima o su familia inmediata. Mustaine y Tewksbury (1999) señalan que el *cyberstalking* es un delito penal motivado por la hostilidad interpersonal y las conductas agresivas derivadas de pretensiones de poder y control. Pittaro (2007) indica que el *cyberstalking* puede estar motivado por la ira, el poder, el control y la rabia que pueden haber sido precipitados por las acciones o inacciones de una víctima.

El discurso del odio *online* es otra forma de acoso *online* basado en la raza, la orientación sexual, el género, la religión, el grupo étnico o la discapacidad que tienen como objetivo promover la hostilidad, la discriminación o la violencia (McDevitt, Levin y Bennett, 2002). Mientras que el *cyberbullying*, el *cyberharassment* y el *cyberstalking* son típicamente llevados a cabo contra un individuo o un grupo pequeño de individuos relacionados, el discurso del odio es considerablemente más amplio, teniendo como objeto a un subgrupo social de la población, o a un grupo de individuos representativos de ese subgrupo.

Los posibles mensajes de discurso de odio en internet son muy diversos. Miró (2016) realizó un interesante estudio clasificatorio a partir del análisis de 250 000 tuits publicados en internet tras los ataques al semanario francés Charlie Hebdo en 2015. Esta

taxonomía incluyó tres categorías generales y cinco tipologías específicas de comunicación violenta y discurso del odio:

1. Discurso referido a la causación de daño físico (incluye la incitación/amenaza directa a la violencia y el enaltecimiento de la violencia física).
2. Discurso que ofende o causa un daño moral personal, incluye los ataques al honor o a la dignidad.
3. Discurso que ofende o causa un daño moral colectivo (incluye la incitación a la discriminación/odio y las ofensas a la sensibilidad colectiva).

Jacks y Adler (2015) distinguen entre diferentes tipos de usuarios que se implican en el discurso del odio *online:*

a) Navegadores *(browsers):* buscan y ven materiales que incluyen mensajes propios del discurso de odio.
b) Comentaristas *(commentators):* se implican con los discursos viéndolos y comentándolos.
c) Activistas *(activists):* añaden material público de odio y buscan promover sus puntos de vista e implicar a otros.
d) Líderes *(leaders):* usan internet para apoyar, organizar y promover sus ideologías extremistas.

Por tanto, los usuarios pueden verse directamente involucrados en el discurso del odio como víctimas o perpetradores, o, indirectamente, como espectadores que se ven expuestos a este tipo de mensajes sin ser personalmente atacados por los comentarios o publicaciones.

2.3. Principales modelos teóricos empleados en la investigación de las distintas formas de ciberacoso

Son diversos los modelos teóricos empleados para explicar la implicación en situaciones de ciberacoso. Entre los posibles marcos explicativos, los más empleados incluyen el modelo general de agresión, la teoría de las actividades cotidianas, la teoría de la elección racional y la teoría del aprendizaje observacional. A continuación, se describen cada uno de estos modelos en relación con el ciberacoso.

No obstante, estos modelos no acotan el conjunto de teorías posibles para explicar el ciberacoso. Así, otros modelos como el ecológico de Bronfenbrenner o el sociocognitivo de procesamiento de la información social podrían aplicarse a la explicación de cualquier conducta agresiva, incluido el ciberacoso. Estos otros modelos serán tratados en el capítulo 5 en relación con el ciberacoso en la pareja.

2.3.1. Modelo general de agresión

El modelo de agresión general (GAM, por sus siglas en inglés) (Anderson y Bushman, 2002) ha sido empleado para explicar los factores personales y situacionales relevantes en las agresiones *online*. Esta teoría proporciona un marco integral para dar cuenta de la conducta agresiva, en general, y del ciberacoso en particular (Kowalski *et al.,* 2014). Asimismo, GAM puede explicar tanto la victimización como la perpetración, puesto que las víctimas y los agresores, con frecuencia, pueden ser la misma persona en situaciones de acoso cibernético (Kowalski *et al.,* 2014).

Siguiendo a Anderson y Bushman (2002), el componente central del modelo son las denominadas estructuras de conocimiento (por ejemplo, las actitudes y los esquemas cognitivos). Estas, que se desarrollan a través de la experiencia, afectan a la percepción, la interpretación, la toma de decisiones y los comportamientos. Las estructuras de conocimiento más relevantes incluyen:

a) *Las actitudes:* creencias valoradas emocionalmente que predisponen a actuar de una determinada manera. Por ejemplo: una creencia relevante en el ciberacoso es la relativa a que la agresión es una forma aceptable de resolver los conflictos.
b) *Los esquemas:* estructuras de conocimiento que facilitan la codificación y la interpretación de la información. Por ejemplo: una persona que tiene un esquema cognitivo sobre los demás como una amenaza podría interpretar sucesos ambiguos como conductas hostiles.
c) *Las expectativas:* estimaciones de aquello que se considera más probable que suceda. Por ejemplo: uno puede esperar que los otros sean agresivos en una determinada situación, lo cual, a su vez, incrementa la probabilidad de llevar a cabo una conducta agresiva.
d) *Los guiones de comportamiento:* esquemas específicos referidos a cómo se debe actuar en situaciones concretas. Un ejemplo de guion de comportamiento incluye la idea de que, ante la agresión de otros, se debe responder también con una agresión.

En la figura 2.1 se presenta un resumen de los principales componentes del modelo. GAM se divide en dos aspectos principales: los procesos distales y los procesos próximos.

Los procesos distales engloban factores biológicos o ambientales que incrementan la probabilidad de la agresión. Los factores biológicos incluyen deterioros en la función ejecutiva o desajustes hormonales (por ejemplo, mayores niveles de testosterona) que se han vinculado con un incremento de la conducta agresiva. Los factores ambientales, por su parte, se refieren a aspectos como criarse en un contexto violento (familia o vecindario), tener un grupo de iguales conflictivo o la exposición a la violencia en los medios de comunicación.

Los procesos próximos explican los episodios individuales de agresión mediante tres etapas: entradas, rutas y resultados.

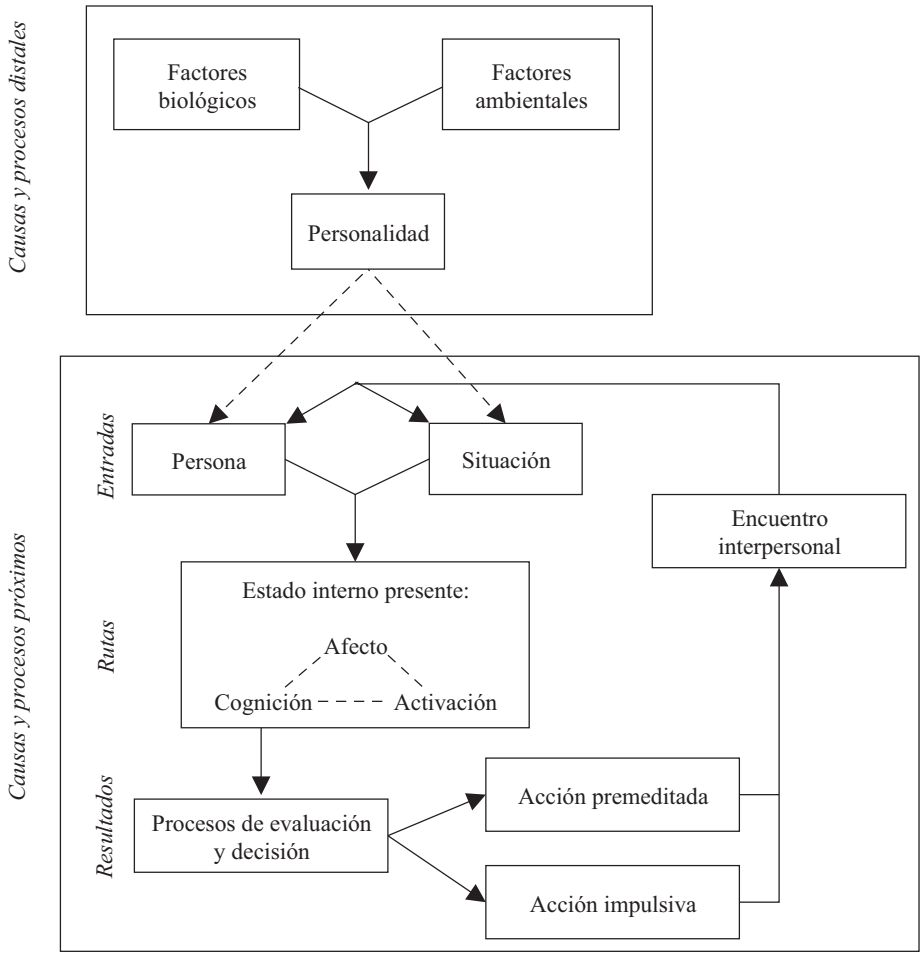

FIGURA 2.1. Resumen del modelo general de agresión.
Fuente: traducido y adaptado de Anderson y Bushman, 2002.

– Las entradas *(inputs)* incluyen factores de la persona y factores situacionales. Los factores de la persona se refieren a variables como el narcisismo, la aceptación de la agresión, la deshumanización de la víctima, el desplazamiento de la responsabilidad, el rasgo de ira, la baja autoestima, el alto neuroticismo o el bajo autocontrol, entre otros. Los factores situacionales engloban aspectos

temporales que pueden incrementar la probabilidad de agresión, tales como la provocación por parte de alguien, la intoxicación por alcohol y drogas, la presencia de un estado de estrés o el anonimato (por ejemplo, en internet), etc.
- Las rutas *(routes)* se refieren a los estados internos presentes en un momento dado que se ven afectados por los factores de la persona y de la situación. Incluyen el estado afectivo (presencia de ira y hostilidad), las cogniciones concretas (por ejemplo, creer que la agresión es adecuada, percibir eventos ambiguos como hostiles, esperar que otros sean agresivos o creer que los conflictos se resuelven con agresión) y el nivel de activación fisiológica (por ejemplo, nerviosismo, cansancio). Estos procesos, además, se influencian mutuamente; por ejemplo, sentir ira puede generar pensamientos de hostilidad hacia alguien, lo cual, a su vez puede incrementar la activación fisiológica (por ejemplo, palpitaciones) y motivar la agresión.
- Resultados *(outcomes)* se centran en los procesos de evaluación y decisión de la situación que resultan en agresión o no agresión. La persona evalúa la situación y decide cómo responder. Como se observa en la figura 2.1, estos procesos pueden dar lugar a una acción impulsiva o premeditada, que conduce a un encuentro interpersonal (agresivo o no).

El encuentro interpersonal influye de nuevo, a través del aprendizaje, en los factores personales y sociales en forma de bucle, iniciando un nuevo ciclo (figura 2.1).

2.3.2. Teoría de la elección racional

La teoría de la elección racional sostiene que los individuos evalúan cada elección de forma racional motivados por la búsqueda del refuerzo y la evitación del dolor o el castigo (Cornish y Clarke, 2014). La figura 2.2 presenta un resumen esquemático de la teoría.

Así, los delitos específicos se producen porque el individuo considera que la conducta antisocial puede proporcionar algún tipo de placer, ventaja, recompensa o gratificación, que supera el coste de la misma. De forma paralela, la teoría establece que el comportamiento puede ser modificado o controlado por el temor o la amenaza de castigo. Por tanto, el miedo al castigo disminuiría la probabilidad de conducta antisocial (Cornish y Clarke, 2014).

De acuerdo con la teoría de la elección racional, si el acto es demasiado arriesgado, las consecuencias negativas para el agresor son probables o el beneficio percibido es pequeño, los individuos optarán por no llevar a cabo la conducta antisocial. Esto implica que es necesario tener en cuenta variables de la persona (por ejemplo, la motivación) y variables situacionales (la presencia de posibles espectadores o penalizaciones por la conducta antisocial). Esta teoría pone el énfasis, por tanto, en que:

1. La conducta antisocial es racional e intencional.
2. Está influida por las necesidades y deseos.
3. La toma de decisiones es específica para cada delito en función su propósito y del potencial beneficio (véase el proceso detallado en la figura 2.2).

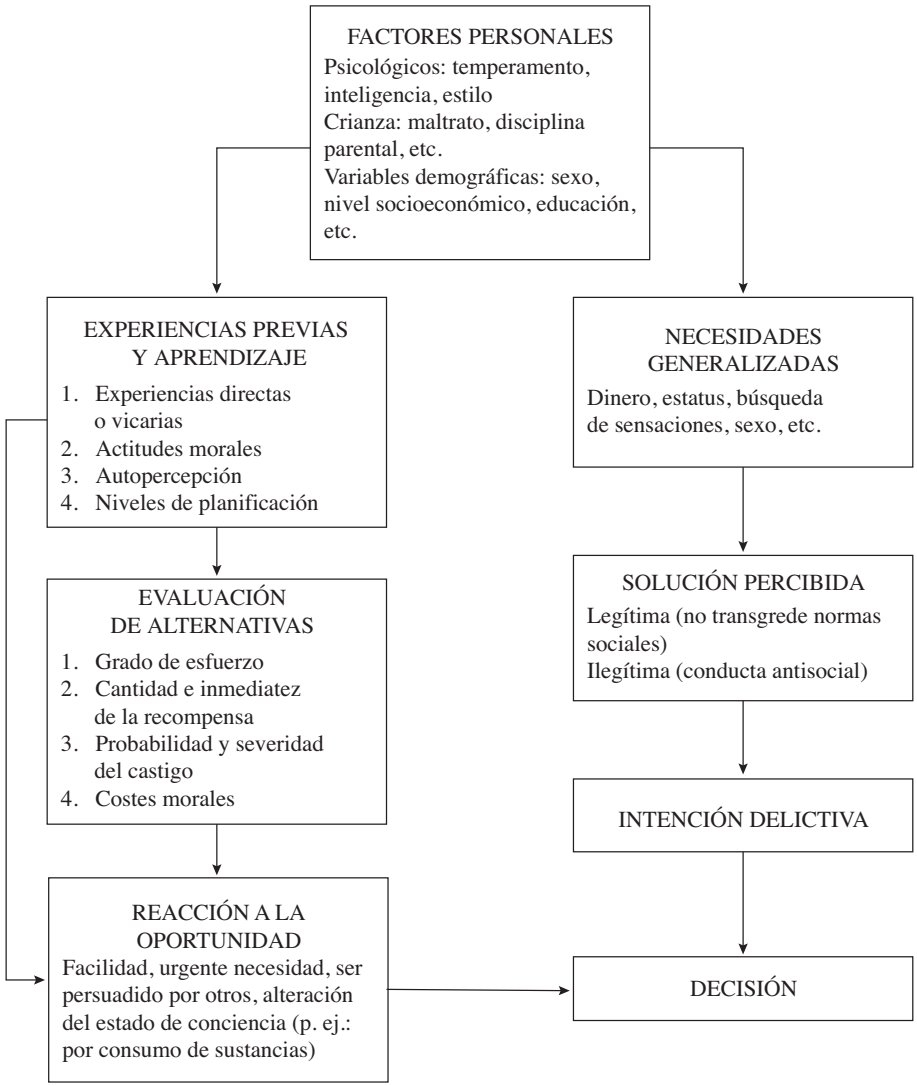

FIGURA 2.2. Representación gráfica de la teoría de la elección racional.
Fuente: traducido y adaptado de Cornish y Clarke, 2014.

Extrapolada al ámbito del ciberacoso, se puede afirmar que las agresiones se basan en una evaluación consciente del beneficio obtenido de agredir *online* a otra persona. Así, el agresor podría pensar que puede obtener algún tipo de beneficio acosando a la víctima por medios electrónicos (por ejemplo, incrementar su estatus, que la víctima acceda a las pretensiones del agresor, satisfacer su deseo de venganza, etc.). La utilidad, sin embargo, puede ser también menos evidente: por ejemplo, el agresor puede experimentar una sensación de venganza al distribuir fotos sin el consentimiento de la víctima o una sensación de superioridad al humillar a alguien de manera anónima. Los potenciales ciberagresores medirían los posibles beneficios y las consecuencias negativas, en base a lo cual elegirían racionalmente. Las consecuencias negativas podrían ser legales (aunque en el mundo virtual las consecuencias legales son poco habituales excepto para delitos muy severos) o podrían castigo por parte de otros (por ejemplo, ser agredido en autodefensa por la víctima).

2.3.3. Teoría de las actividades cotidianas

De acuerdo con la teoría de las actividades cotidianas (Cohen y Felson, 1979), es probable que ocurra un delito o conducta antisocial como el ciberacoso, cuando convergen tres elementos esenciales en el espacio y el tiempo (Navarro y Jasinski, 2013).

El primero es la presencia de un agresor motivado. Los agresores motivados son individuos dispuestos y capaces de cometer actividades delictivas o antisociales. La teoría asume que cualquier persona que tenga la oportunidad y esté motivada para ello puede implicarse en una conducta antisocial.

La segunda condición es la presencia de una víctima particularmente vulnerable o atractiva para el agresor. La teoría supone un papel relevante a las víctimas, puesto que las diferentes conductas de riesgo pueden incrementar la vulnerabilidad a ser victimizadas. En el caso del ciberespacio, una persona vulnerable emocionalmente (por ejemplo, deprimida), un menor de edad (por ejemplo, en situaciones de *online grooming*) o una persona que se implique en conductas de riesgo (como enviar fotos íntimas) se encuentran en una situación de riesgo para ser víctima de ciberacoso.

El tercer elemento es la ausencia de un guardián eficaz que proporcione protección y disuada de cometer la conducta. Este tercer componente se refiere a los controles sociales que puedan castigar al agresor o proteger a la víctima y, por tanto, evitar que tenga lugar la conducta antisocial. Por ejemplo, la ausencia de controles parentales sobre el uso de las TIC o la ausencia de internautas concienciados que intervengan protegiendo a la víctima o sancionando al agresor son factores que pueden influir en el ciberespacio.

En definitiva, la teoría relaciona el delito con los estilos de vida que las personas mantienen, los cuales las ponen en una situación de riesgo ante los posibles agresores dispuestos.

2.3.4. Teoría del aprendizaje social

La teoría del aprendizaje social de Bandura plantea que las personas aprenden en parte imitando modelos (Bandura, 1978). Así, los cambios en el comportamiento, la cognición o el estado emocional son el resultado de observar el comportamiento de otra persona o las consecuencias de ese comportamiento.

Posteriormente, Bandura incorporó la cognición a sus ideas sobre el aprendizaje social, una modificación que se conoció como teoría sociocognitiva (por ejemplo, Bandura, 2001). La teoría sociocognitiva incluye los efectos de los procesos cognitivos (juicios, motivación, etc.), en el comportamiento de un individuo y en el entorno que lo influye. Las personas buscan desarrollar un sentido de competencia personal y ejercer control sobre eventos en sus vidas, un sentido que se ve afectado por factores cognitivos como su autoeficacia, sus expectativas de resultados, sus objetivos y su autoevaluación. En lugar de ser un receptor pasivo de los estímulos ambientales, las personas influyen activamente en su aprendizaje al interpretar los resultados de sus acciones, lo cual a la postre afecta a su entorno y a los propios factores personales. De hecho, el énfasis en la interacción de factores conductuales, ambientales y personales es un aspecto fundamental de la teoría.

La teoría del aprendizaje observacional ha sido empleada para explicar la participación en el ciberacoso y en el discurso de odio *online*. Así, diversas investigaciones sobre ciberacoso han mostrado que ser espectadores incrementa la desconexión moral (deshumanización de la víctima, minimización de las consecuencias, difusión de la responsabilidad, etc.) y las actitudes negativas hacia las víctimas, al tiempo que reducir la empatía hacia la víctima (Pabian *et al.,* 2016), lo cual incrementa la probabilidad de convertirse en agresor.

Por otra parte, el discurso del odio a menudo se lleva a cabo con el objetivo de influir en los valores de un grupo de iguales y establecer la identidad del grupo (Blaya y Audrin, 2019). Cuando los adolescentes observan que sus iguales difunden el odio *online* pueden aprender que este es un comportamiento apropiado y útil para aumentar su estatus y aceptación. Así, los espectadores podrían ser más propensos a unirse y compartir, publicar o enviar material de odio contra grupos sociales. En línea con la teoría, existe evidencia empírica que demuestra que los individuos tienden a usar expresiones más agresivas en su comunicación e interacción *online* cuando observan que sus iguales se comportan agresivamente (Pabian *et al.,* 2016).

2.4. Prevalencia, factores de riesgo y protección

Recientemente, diversos autores han debatido si la incidencia del ciberacoso está en aumento o si se ha estabilizado. Algunos especialistas han sugerido que, con los continuos

cambios tecnológicos, las tasas de prevalencia del acoso cibernético están aumentando. Sin embargo, otros autores argumentan que la incidencia del acoso cibernético no ha aumentado en los últimos años, más bien se ha trasformado en función del contexto tecnológico cambiante (Kowalski *et al.,* 2014). Lo que parece incuestionable, desde un punto de vista epidemiológico, es que las tasas de ciberacoso son elevadas, como se comprobará a continuación.

2.4.1. Prevalencia del ciberacoso

Con considerables diferencias entre los estudios, las estimaciones de prevalencia del ciberacoso han oscilado entre el 10 y el 40% (Garaigordobil, 2011; Kowalski *et al.,* 2014). En una revisión de metaanálisis de los estudios que se habían llevado a cabo, Modecki, Minchin, Harbaugh, Guerra y Runions (2014) encontraron una prevalencia media del 15% tanto para la victimización como para la perpetración de ciberacoso (frente una tasa, aproximadamente, del 35% para el *bullying* tradicional). En otra revisión, Hamm (2015) informó de una prevalencia media del 15% para la victimización y del 23% para la perpetración.

En España, el 24% de los adolescentes reconoce haber sufrido un incidente de *cyberbullying,* el 16% dos incidentes, el 8% tres y el 4% cuatro o más (Gámez-Guadix, Orue, Smith y Calvete, 2013). Algunas experiencias de ciberacoso tienden a cronificarse. Aproximadamente el 6% de los adolescentes son víctimas estables de ciberacoso durante un periodo de al menos un año (Gámez-Guadix, Gini y Calvete, 2015).

En otro estudio en España, Montiel, Carbonell y Pereda (2016) analizaron la prevalencia de diferentes formas de ciberacoso entre adolescentes. La prevalencia del *online harassment* (amenazas repetidas u otros comportamientos ofensivos para avergonzar o humillar enviados o publicados *online* para que otros lo vean, independientemente de la edad del autor) fue del 50%, siendo significativamente más prevalente entre las chicas y entre adolescentes mayores.

La investigación sobre la prevalencia de diferentes formas de participación en el discurso del odio sugiere que la forma más común de experimentarlo es presenciarlo como espectadores. Por ejemplo, en un estudio con 3500 adolescentes y adultos jóvenes de cuatro países, aproximadamente el 53% de los estadounidenses, el 48% de los finlandeses, el 39% de los británicos y el 31% de los alemanes dijeron haber presenciado discurso del odio. En el mismo estudio, el 16% de los participantes estadounidenses, el 10% de los finlandeses, el 12% de los británicos y el 4% de los alemanes confesaron haber sido atacados personalmente por mensajes propios del discurso de odio (Hawdon, Oksanen y Räsänen, 2015). Más recientemente, un estudio con participantes franceses de entre 11 y 20 años concluyó que alrededor del 57% de estos estaban expuestos al odio *online,* aproximadamente el 10% fueron víctimas de odio en redes sociales y el 5% publicó o compartió material de odio *online* (Blaya y Audrin, 2019).