Acoso cibernético (ciberacoso)

Derecho nacional y comparado

Autora

Christine Weidenslaufer

cweidenslaufer@bcn.cl

SUP: 134458

Resumen

Aunque se trata de un concepto nuevo y cuya definición no es uniforme en la doctrina ni en la legislación extranjera, el ciberacoso o acoso cibernético puede definirse, a grandes rasgos, como el acoso realizado por medios tecnológicos y/o en dispositivos digitales y que a menudo está dirigido a mujeres y niñas.

El ciberacoso se enmarca en un fenómeno más amplio, la ciberviolencia, que abarca una amplia variedad de delitos (v.gr. diferentes tipos de acoso, violación de la privacidad, abuso y explotación sexual y delitos contra grupos sociales o comunidades específicas). Entre las formas de ejercer el acoso se encuentran las amenazas de violencia (incluyendo la violencia sexual), la coerción, los insultos o amenazas, la incitación a la violencia, la porno venganza, la incitación al suicidio o a las autolesiones.

En Chile, diversos tipos penales sobre acoso (general, sexual, laboral, escolar) contemplan medios tecnológicos para su comisión. Sin embargo, no existiría una figura penal específica de ciber acoso, como la referida en el proyecto de ley sobre violencia digital (boletín N° 13.928-07), en actual tramitación.

De la revisión de la legislación sobre ciber acoso en EE.UU., España y México, todos con normas específicas para sancionar esta conducta y demás relacionadas, se destacan los siguientes aspectos:

- Respecto al tipo penal, Estados Unidos en su legislación federal cuenta con varios tipos penales aplicables a conductas de acoso a través de sistemas de comunicaciones. A nivel estadual, California, utiliza la fórmula general “medios de comunicación electrónica” junto con un listado abiertos de ejemplos; y en la normativa de Illinois se sanciona en forma especial la instalación de software de monitoreo electrónico o la creación o mantención de sitios web destinados a amenazar a la víctima del acoso. En España, en cambio, si bien existe un delito de ciberacoso, este está dentro del delito de amenazas, y su comisión por medios de comunicación representa un agravante. Por último, México (estado de México), el ciberacoso incluye explícitamente, como una de las hipótesis de comisión del delito, que éste tenga por objeto concertar un encuentro o acercamiento físico con la víctima.
- Por su parte, las sanciones previstas varían de un país a otro: EE.UU, multa y/o pena de prisión desde uno a 20 años, dependiendo de la gravedad de la conducta; España: tres meses a dos años de prisión o multa; y México: uno a ocho años de prisión y multa.

Introducción

Según la Encuesta Nacional de Ciberacoso y Salud Mental 2021 (Segegob, 2021) -citada por información de prensa-, un 47% de los jóvenes de entre 15 a 29 años afirma haber sido víctima de violencia digital en los últimos tres meses y un 64% consigna haber sido testigo de esta práctica. De esos jóvenes ciberacosados, un 38% declara presentar síntomas que son compatibles con depresión mayor; un 25% afirma que ante episodios de ciberacoso su reacción es hacerse daño, y un 69% señala que el ciberacoso del que son víctimas consiste en comentarios hirientes o malintencionados en línea[1].

A solicitud del usuario, se revisa legislación extranjera sobre ciberacoso, en el marco del actual Proyecto de ley que proscribe, tipifica y sanciona la violencia digital en sus diversas formas y otorga protección a las víctimas de la misma (boletín N° 13.928-07), actualmente en primer trámite constitucional en la Comisión de Seguridad de la Cámara de Diputadas y Diputados.

Este informe se divide en tres partes. En la primera se conceptualiza el ciberacoso y las demás conductas relacionadas en el contexto de la violencia digital en la doctrina y el derecho, en la segunda se analiza la legislación penal sobre el ciberacoso en Estados Unidos, España y México y en la tercera se analiza el proyecto de ley chileno sobre violencia digital en relación a los tipos penales quer ella consagra, a la luz del derecho comparado.

El informe aborda el ciberacoso sin calificación de sujetos, es decir, entre personas de todas edades y sexos[2]. Este informe incluye información actualizada contenida en los informes BCN “Acoso Cibernético (Ciberbullying)” de Pamela Cifuentes, Guido Williams y Mauricio Holz (2018) y “Ciberacoso: normativa penal en el derecho comparado” de Annette Hafner y Christian Finsterbusch (2012).

Se advierte que las regulaciones consultadas en general utilizan el masculino como término no marcado[3]. Así, cuando se utiliza el término “acosador”, entre otros, se incluye también al género femenino, es decir, a la “acosadora”. Se excepcionan los casos donde se distingue explícitamente en la norma entre el género femenino y masculino.

Las traducciones son propias.

I. Conceptualización del ciber acoso

1. Definición general

Como otros vocablos de nueva cuña, el ciberacoso no cuenta con una única definición. Es por ello que a continuación se detallan algunas conceptualizaciones recogidas en el extranjero:

[1] Segegob (2021).
[2] El ciberacoso entre menores, que puede tener regulación distinta, no forma parte del presente informe.
[3] Según la RAE (s/f), "el uso genérico del masculino se basa en su condición de término no marcado en la oposición masculino / femenino".

De acuerdo al sitio gubernamental norteamericano *stopbullying.gov*, el ciberacoso (*cyberbullying*) es, en breves palabras, el Proyecto de ley que proscribe, tipifica y sanciona la violencia digital en sus diversas formas y otorga protección a las víctimas de la misma (boletín N° 13.928-07), tales como teléfonos celulares, computadoras y tabletas. El ciberacoso, señala el mismo sitio, incluye enviar, publicar o compartir contenido negativo, perjudicial, falso o cruel sobre otra persona, incluyendo su información personal o privada, provocándole humillación o vergüenza. Algunos acosos por Internet constituyen conductas penales[4].

Los medios para cometer esta conducta incluyen mensajes de texto (vía correo electrónico) y aplicaciones de mensajería instantánea en dispositivos móviles y tabletas, o bien por Internet, en las redes sociales (por ej. Facebook, Instagram, Snapchat y Tik Tok), foros en Internet, salas de chat y tableros de mensajes, como Reddit, o de juegos en línea, donde las personas pueden ver, participar o compartir contenido[5].

Para el Servicio de Investigación del Parlamento Europeo (EPRS, por sus siglas en inglés, 2018), el ciberacoso es el acoso verbal o psicológico llevado a cabo a través de medios electrónicos de comunicación, generalmente de forma repetitiva y principalmente a través de las redes sociales. De acuerdo al EPRS, el ciberacoso puede tomar varias formas, como insultos, amenazas e intimidación, chismes, exclusión, acoso o robo de identidad.

2. Ciberviolencia y conductas relacionadas

No obstante las definiciones generales ya enunciadas, debe considerarse que el ciberacoso se enmarca en un fenómeno mayor, cual es, la ciberviolencia. Esta última abarca diversas conductas y delitos, y, al igual que en el caso del ciberacoso, se trata de un término difícil de definir con precisión, que suele confundirse con otros términos relacionados o similares, como se verá más adelante.

El Grupo de Trabajo de T-CY sobre ciberacoso y otras formas de violencia[6], del Consejo de Europa[7], en su Estudio de Mapeo de la Ciberviolencia (*Mapping study on cyberviolence*) de 2018 -en adelante, el Estudio 2018-, la definió como “el uso de sistemas informáticos para causar, facilitar o amenazar con violencia contra individuos, que resulte (o pueda resultar) en daño o sufrimiento físico, sexual, psicológico o económico y puede incluir la explotación de las circunstancias, características o vulnerabilidades del individuo”[8].

[4] Stopbullying.gov (2021).
[5] Stopbullying.gov (2021).
[6] Cybercrime Convention Committee (T-CY), Working Group on cyberbullying and other forms of online violence, especially against women and children.
[7] El Consejo de Europa, con sede en Estrasburgo (Francia), es una organización intergubernamental de la que forman parte 47 Estados europeos.
[8] El informe citado aclara que “es fundamental recordar que muchas formas de violencia cibernética ya están contempladas en el derecho nacional o internacional por las disposiciones del “mundo físico”, y es posible que las investigaciones no tengan que esperar a una nueva legislación. Por ejemplo, cuando las computadoras se utilizan para causar o facilitar la violencia a través de la transmisión de mensajes que causan daño psicológico, o a través de anuncios de asesinato, violación, secuestro o trata de seres humanos, estos casos pueden ser procesados (dependiendo de sus hechos) como agresión, violación de la privacidad, amenaza ilegal, extorsión, solicitud de violación o asesinato, distribución ilegal de contenido (como fotografías), violencia doméstica, etc. Además, dada

En la práctica, continúa el Estudio 2018, los actos de ciberviolencia pueden implicar diferentes tipos de acoso, violación de la privacidad, abuso y explotación sexual y delitos contra grupos sociales o comunidades específicas. La ciberviolencia también puede implicar amenazas directas o violencia física, así como diferentes formas de ciberdelincuencia.

Si bien todavía no existe un léxico o tipología estable de los delitos considerados ciberviolencia, y muchos de los ejemplos de tipos de ciberviolencia están interconectados, se superponen (o se utilizan como sinónimos) o consisten en una combinación de actos, el Estudio 2018 del Consejo de Europa agrupa estas conductas criminales en las siguientes categorías: a) acoso en sentido amplio (*cyberharassment*), b) cibercrimen (*cybercrime*), c) explotación y abuso sexual de niños en línea (*Online sexual exploitation and sexual abuse of children*), d) amenazas directas o violencia física relacionadas con las TIC[9] (*ICT-related direct threats of or physical violence*), e) delitos de odio relacionados con las TIC (*ICT-related hate crime*) y f) violaciones de la privacidad relacionadas con las TIC (*ICT-related violations of privacy*)[10]. A su vez, cada categoría agrupa otras conductas, como se observa a continuación[11]:

a) Acoso en sentido amplio (*cyberharassment*)

Este concepto agrupa la difamación y otros daños a la reputación, y el ciberacoso en sentido específico (*cyberbullying*, principalmente en el contexto escolar) las amenazas de violencia (incluyendo la violencia sexual), la coerción, los insultos o amenazas, la incitación a la violencia, la porno venganza, la incitación al suicidio o a las autolesiones, etc. Ejemplos de acoso cibernético incluyen mensajes de texto o correos electrónicos desagradables, rumores enviados por correo electrónico o publicados en sitios de redes sociales e imágenes, videos o sitios web vergonzosos por una sola persona o por un grupo de personas, para causar vergüenza a la víctima o algo peor entre amigos, familiares o compañeros de trabajo.

El acoso cibernético (en sentido amplio) es quizás la forma más amplia de ciberviolencia e implica un curso de conducta persistente y reiterada, diseñada y dirigida hacia una persona específica y que causa angustia emocional severa y, a menudo, miedo a sufrir un daño físico. Los ciber acosadores se hacen pasar por víctimas en anuncios en línea y sugieren, falsamente, que sus víctimas están interesadas en tener relaciones sexuales con extraños. A veces, los acosadores manipulan los motores de búsqueda para asegurar la prominencia de las mentiras en las búsquedas de los nombres de las víctimas, invaden la privacidad de las éstas al publicar su información confidencial, como imágenes de desnudos o números de identidad personal, o bien pueden usar la tecnología para desconectar a las víctimas.

---

la dependencia de los sistemas informáticos -incluida la dependencia psicológica, física y económica- algunos tipos de cibercrímenes (acceso ilegal a datos personales íntimos, destrucción de datos, etc.) también pueden ser considerados actos de ciberviolencia" (Council of Europe, 2018:5).

[9] TIC: tecnologías de la información y las comunicaciones.

[10] Council of Europe (2018:6).

[11] Council of Europe (2018:6-7).

El acoso cibernético, señala el Estudio 2018, en el discurso popular puede describirse o estar relacionado con la "pornografía de venganza" o la "sextorsión"[12]. Este tipo de acoso a menudo está dirigido a mujeres y niñas y se denomina "ciberviolencia contra mujeres y niñas" (*cyber violence against women and girls, CVAWG* o *Cyber VAWG*) que involucra: correos electrónicos u otros mensajes sexualmente explícitos no deseados; avances ofensivos en redes sociales y otras plataformas; amenaza de violencia física o sexual; discurso de odio: lenguaje que denigra, insulta, amenaza o ataca a una persona en función de su identidad (género) y/u otros rasgos (como orientación sexual o discapacidad).

En particular, se distingue el *cyberbullying* como una forma de acoso cibernético que tiende a asociarse con víctimas que son niños, a menudo en edad escolar secundaria, mientras que fenómenos como el acecho cibernético (*cyberstalking*) y la sextorsión/"pornografía de venganza" se asocian más a adultos o adultos jóvenes. Los límites entre estos conceptos no son claros y ni tampoco hay acuerdo sobre cuándo usar qué término.

Finalmente, señala el estudio en comento, no todas las formas de *cyberbullying* constituyen delito, pues éste puede considerarse como un término paraguas para muchas actividades de acoso en línea, algunas de las cuales son más graves que otras. La literatura identifica diferentes tipos de *cyberbullying*, que incluyen la denigración, la participación en grupos de exclusión/chismes, la falsificación/suplantación de identidad para publicar contenido en línea, *cyberstalking*, *outing*[13], *phishing*[14], *sexting*[15], entre otras acciones. Estas acciones pueden dar lugar a manipulación sexual, creación y distribución no consentida de imágenes o vídeos íntimos, autolesiones (*cutting*) y suicidio. Por ello, desde una perspectiva de investigación y persecución penal, es fundamental distinguir entre los diferentes tipos de ciberacoso y también es importante distinguir entre los diferentes roles que juegan los individuos en un determinado acto de ciberacoso.

b) Cibercrimen

Incluye delitos del espacio digital, como el acceso ilegal, la interceptación ilegal, la interferencia de datos, la interferencia de sistemas, la falsificación informática, el fraude informático y la pornografía infantil.

c) Explotación y abuso sexual de niños en línea

Incluye el abuso sexual, la prostitución infantil, la pornografía infantil, la corrupción de menores de edad, la solicitación de niños con fines sexuales, el abuso sexual a través de transmisiones en vivo (*live streaming*), etc.

---

[12] Sextorsión es un término en el discurso popular que engloba actividades que (a) implican manipulación o coerción para realizar actividades sexuales en beneficio del agresor y/o crear imágenes sexualmente explícitas de la víctima y (b) el delito tradicional de extorsión (Council of Europe, 2018:11).

[13] *Outing* es la revelación de la orientación sexual o identidad de género de una persona LGBT sin su consentimiento.

[14] *Phishing* es la práctica fraudulenta de enviar correos electrónicos que pretenden ser de empresas acreditadas para inducir a las personas a revelar información personal, como contraseñas y números de tarjetas de crédito.

[15] *Sexting* es la acción o práctica de enviar fotografías o mensajes sexualmente explícitos a través del teléfono móvil.

d) Amenazas directas o violencia física relacionadas con las TIC

Agrupa delitos como el homicidio, el secuestro, la violencia sexual, la violación, la tortura, la extorsión, el chantaje, el *swatting*[16], la incitación a la violencia, ataques a infraestructura crítica, automóviles o dispositivos médicos que causan lesiones o muerte, entre otros.

e) Delitos de odio relacionados con las TIC

Se trata de delitos contra grupos basados en la raza, la etnicidad, la religión, el sexo, la orientación sexual, la discapacidad, etc.

f) Violaciones de la privacidad relacionadas con las TIC

Se encuentran aquí las intrusiones informáticas; el tomar, compartir, manipular datos o imágenes, incluyendo datos íntimos; la extorsión sexual o "sextorsión", el acecho cibernético (*cyberstalking*), la búsqueda y difusión de datos personales (*doxing*), el robo y la suplantación de identidad, etc.

Finalmente, para efectos de la materia en estudio, se destaca el caso de México, cuya Ley General de Acceso de las Mujeres a una Vida Libre de Violencia distingue, en su Capítulo IV ter adicionado en junio de 2021, dos modalidades de violencia en el contexto de las telecomunicaciones: digital y mediática.

> ARTÍCULO 20 Quáter.- **Violencia digital** es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.
>
> Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación.
>
> Para efectos del presente Capítulo se entenderá por Tecnologías de la Información y la Comunicación aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos.
>
> La violencia digital será sancionada en la forma y términos que establezca el Código Penal Federal. [el destacado es nuestro]

> ARTÍCULO 20 Quinquies.- **Violencia mediática** es todo acto a través de cualquier medio de comunicación, que de manera directa o indirecta promueva estereotipos sexistas, haga apología de la violencia contra las mujeres y las niñas, produzca o permita la producción y difusión de discurso

[16] Se llama *swatting* al uso de teléfonos y, a menudo, de sistemas informáticos, para engañar a un servicio de emergencia con el fin de enviar a las fuerzas del orden público a un lugar específico basándose en un reporte falso (Council of Europe, 2018:14).

> de odio sexista, discriminación de género o desigualdad entre mujeres y hombres, que cause daño a las mujeres y niñas de tipo psicológico, sexual, físico, económico, patrimonial o feminicida.
>
> La violencia mediática se ejerce por cualquier persona física o moral que utilice un medio de comunicación para producir y difundir contenidos que atentan contra la autoestima, salud, integridad, libertad y seguridad de las mujeres y niñas, que impide su desarrollo y que atenta contra la igualdad. [el destacado es nuestro]

II. Regulación del cibercacoso en el Derecho comparado

Los gobiernos, la sociedad civil, el sector privado y las organizaciones internacionales cada vez más adoptan políticas y medidas para abordar la ciberviolencia. El enfoque principal es la prevención y la educación dirigida a niños y adultos jóvenes[17].

Sin embargo, señala el Estudio 2018, la respuesta del derecho penal a otras formas específicas de ciberviolencia no ha sido homogénea. Además de la tipificación como delito de los actos relacionados con la explotación sexual infantil y el abuso sexual, las disposiciones legales específicas relativas a otras formas de ciberviolencia son menos comunes.

Algunos países que han tipificado como delito el ciberacoso (con distintas denominaciones, tales como *cyberharassment, cyberstalking* y *cyberbullying*), separadamente de los delitos que constituyen formas de coerción, amenazas, acoso (sexual), violaciones de la privacidad, insultos, extorsión y otras formas de violencia, incluidas la xenofobia, el racismo y otras formas de incitación al odio que también pueden aplicarse cuando están involucrados sistemas informáticos.

Algunas formas de ciberviolencia pueden imputarse utilizando éstas y otras leyes del mundo físico (como la incitación a cometer un delito).

1. Estados Unidos (EE.UU.)

A nivel federal, el US Code (USC)[18] contiene diversas normas aplicables al ciberacoso. No obstante, este marco sólo es aplicable en comunicaciones de acosos interestatales o con el extranjero, ya que el ciberacoso dentro de un mismo estado está sujeto a la legislación estatal.

A modo de ejemplo, las siguientes normas son aplicables a hipótesis de acoso cibernético:

- 18 USC 875 (c) y (d) (Amenazas en la comunicación interestatal): sanciona a quien transmite, en el comercio interestatal o extranjero, cualquier tipo de comunicación conteniendo amenazas

[17] Council of Europe (2018:40).

de secuestrar a una persona, extorsionarla, destruir su reputación, de dañar la propiedad o la reputación de una persona muerta, o de hacer otro tipo de daño, con una pena de hasta 20 años.

- 47 USC 223 (Llamadas obscenas o acosadoras): sanciona a quien, en la comunicación interestatal o extranjera, utilice un sistema de telecomunicaciones para molestar, acosar, amenazar o abusar a alguna persona de manera anónima, con hasta 2 años de prisión y/o multa. Esta norma solamente se aplica a la comunicación directa y en caso de que el agresor se mantenga anónimo.

- 18 USC 2261A (Acoso, *stalking*): sanciona a quien acosa, mediante correo, e-mail o internet a una persona, con la intención de matar o hacer daño esta última, o de causar en ella o en un familiar el temor de muerte o de daño serio corporal, sancionándolo con multa y una pena de prisión de hasta 5 años; por no más de 20 años si la víctima sufre una desfiguración permanente o lesiones corporales que amenazan la vida; por no más de 10 años, si la víctima sufre lesiones corporales graves o si el acosador usa un arma peligrosa durante el delito; y prisión perpetua, en casos de muerte.

Si bien los estados tienen leyes penales que se aplican para el acoso, no todos tienen estatutos especiales en materia de acoso cibernético. A continuación, se exponen tres ejemplos de dichas legislaciones estaduales:

a) California

El artículo 653m del Código Penal californiano sanciona a quien, con la intención de molestar, llama por teléfono o contacta mediante un medio de comunicación electrónica (teléfonos, teléfonos celulares, computadoras, grabadoras de video, máquinas de fax, buscapersonas, asistentes digitales personales, teléfonos inteligentes y cualquier otro dispositivo que transfiera signos, señales, escritura, imágenes, sonidos o datos) a otra persona, dirigiéndole a ella o a su familia palabras ofensivas o amenazándola de dañarla tanto corporal como patrimonialmente.

La pena para estas conductas es prisión por hasta 1 año.

La misma sanción se contempla para quien, con la intención de molestar o acosar, llama repetidas veces por teléfono o contacta repetidas veces a otra persona por medios electrónicos, o por una combinación de ambos.

El artículo 646.9 del Código Penal, por su parte, dispone que comete el crimen de acoso (*stalking*) quien, de manera intencional, malintencionada y repetidamente persigue a otra persona o la acosa, y que hace una amenaza seria con la intención de causar en ella temor justificado por su seguridad o la de su familia.

Se sanciona con una pena de prisión de hasta un año, o multa de 1.000 dólares, que en casos graves podrá aumentarse hasta 5 años.

b) Illinois

Según la sección 12-7.5 de la legislación criminal[19], una persona comete el delito de ciberacoso (*cyberstalking*) cuando usa la comunicación electrónica, dirigiéndose a una persona específica, sabiendo o debiendo saber que su comportamiento causa en ella temor por su seguridad o estrés emocional.

Asimismo, se entiende que una persona comete ciberacoso si él o ella, a sabiendas y sin justificación legal, cuando:

i. en al menos 2 ocasiones separadas, acosa a otra persona mediante el uso de la comunicación electrónica; ó
ii. instala o coloca software de monitoreo electrónico o spyware en un dispositivo de comunicación electrónica como un medio para acosar a otra persona; ó
iii. crea subrepticiamente y mantiene un sitio web durante al menos 24 horas que es accesible a terceras personas y que contiene frases acosadoras y amenazas; y:
   - transmite amenazas de daño físico inmediato o futuro, agresión sexual, confinamiento o restricción a esa persona o un miembro de su familia; o
   - hace temer razonablemente a esa persona o a un familiar suyo de daño físico inmediato o futuro, agresión sexual, confinamiento o restricción; o
   - en cualquier momento, a sabiendas, solicita a un tercero la comisión de un acto ilegal hacia esa persona o un miembro de su familia.

Para todos estos casos, la sanción es prisión de uno a tres años y una pena de 25.000 dólares. Si hay reincidencia la pena va de dos a cinco años.

2. España

En España, el ciberacoso está regulado en los tipos penales generales del Código Penal. En particular, el artículo 172 ter sanciona a quien acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

- La vigile, la persiga o busque su cercanía física.
- Establezca o intente establecer contacto con ella **a través de cualquier medio de comunicación**, o por medio de terceras personas.
- 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.
- Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Este delito se castiga con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses.

[19] Illinois Statutes Chapter 720. Criminal Offenses §-7.5.Cyberstalking.

Por otra parte, el artículo 169 regula el delito de amenaza. La norma dispone que quien amenaza a otro con causarle a él, a su familia o a otras personas con las que esté íntimamente vinculado un mal que constituya delitos de homicidio, lesiones, aborto, contra la libertad, torturas y contra la integridad moral, la libertad sexual, la intimidad, el honor, el patrimonio y el orden socioeconómico, será castigado con una pena de prisión máxima de 5 años.

La comisión del delito por medios de comunicación representa un agravante, pues las penas se impondrán en su mitad superior si las amenazas se hicieren por escrito, por teléfono o **por cualquier medio de comunicación o de reproducción**, o en nombre de entidades o grupos reales o supuestos. Además, se pueden aplicar, según el caso:

- El delito de la infracción al derecho de la intimidad, por ejemplo revelando secreto de personas a través de invasión de documentos electrónicos o intercepción de comunicación electrónica (artículos 197 al 219).
- Las normas relativas al delito de calumnias e injurias, al referirse a si éstas se propagan con publicidad, por ejemplo a través de redes sociales, foros o correos electrónicos (artículos 205 al 216).

Las penas de estos delitos van desde uno hasta siete años de prisión y/o multa.

3. México

Este país no cuenta con una ley federal sobre la materia. A nivel estadual, a modo de ejemplo, se observa que la reforma del año 2021, que incorporó el “Capítulo VI, Violencia ejercida a través de las tecnologías de la información y la comunicación” al Código Penal del Estado de México, si bien no lo denomina explícitamente ciberacoso, tipifica conductas directamente relacionadas con éste en el ámbito de la violencia sexual. Así, se sanciona:

- A quien reciba con consentimiento contenidos audiovisuales de naturaleza erótico, sexual o pornográfico y los comparta sin consentimiento de la víctima, a través de cualquier tecnología de la información y comunicación, se le impondrá de 1 a 5 años de prisión y multa económica que va de $17,376 - $43,400 pesos mexicanos aproximadamente. La misma pena se aplica a quien reciba del receptor original tales contenidos o los encuentre por su cuenta, y los difunda sin consentimiento de la persona que aparece en ellos (artículo 211 Ter).
- A quien coaccione, intimide, hostigue, exija o engañe a otra persona para elaborar contenidos eróticos, sexuales o pornográficos bajo la amenaza de publicar o compartir material de la misma naturaleza (obtenido de la víctima anteriormente o por cualquier otro medio), sin su consentimiento, o bien con la finalidad de concertar un encuentro o acercamiento físico, se le impondrá de 3 a 7 años de prisión y una multa económica que va de $17,276 a $34,752 pesos mexicanos aproximadamente. Si el encuentro tiene por objeto obtener concesiones de índole sexual o material audiovisual con contenido explícito, se le impondrá de cuatro a ocho años de prisión (artículo 211 Quater).

- Las sanciones de los dos artículos anteriores se agravan hasta el doble si se cometen en contra de una persona menor de 18 años o que no tenga la capacidad de comprender el significado del hecho (artículo 211 Quinquies).

Las agravantes para estos delitos son las siguientes:

- Que el victimario hubiera tenido algún vínculo con la víctima (cónyuge, conviviente o haya tenido alguna relación sentimental, afectiva, de confianza, laboral o análoga con la víctima).
- Que el victimario haya cometido la conducta con fines lucrativos o en su calidad de servidor público y haya obtenido, sin consentimiento y por cualquier medio, contenido erótico, sexual, de actos íntimos, interpersonales, efectuados en lugar privado y lo publique.
- Que el delito se cometa en contra de un(a) menor de edad o una persona que no tenga la capacidad de comprender el significado del hecho.
- Que para la obtención del contenido sexual, la víctima se encuentre en estado de ebriedad o bajo el influjo de drogas.

Por último, el Código Penal regula, en forma separada, los delitos de hostigamiento sexual (art. 269) y acoso sexual (art. 270).

III. Regulación del acoso y el ciberacoso en Chile

La legislación chilena ha definido el acoso en contextos particulares, incluso contemplando el uso de medios tecnológicos para su comisión, como se analiza a continuación. A la luz de los mismos se analiza proyecto de ley sobre violencia digital, que consagra, entre otros tipos penales, el acoso digital.

1. El delito de acoso en sus distintas variantes

En nuestro país, el acoso cibernético no está regulado, tal como se encuentra definido a nivel internacional. Sin embargo, el delito de acoso si lo está en algunos ámbitos específicos del mundo físico y que contemplan también el uso del espacio digital para cometerlos.

Esto ocurre con la Ley N° 20.536 de violencia escolar, del año 2011, que incorporó a la Ley General de Educación el artículo 16 B, norma que define el “acoso escolar”. En dicho texto, los medios tecnológicos son considerados como una de las herramientas que puede usarse para cometer una agresión u hostigamiento entre estudiantes:

> Artículo 16 B. Se entenderá por **acoso escolar** toda acción u omisión constitutiva de agresión u hostigamiento reiterado, realizada fuera o dentro del establecimiento educacional por estudiantes que, en forma individual o colectiva, atenten en contra de otro estudiante, valiéndose para ello de una situación de superioridad o de indefensión del estudiante afectado, que provoque en este último, maltrato, humillación o fundado temor de verse expuesto a un mal de carácter grave, ya sea **por medios tecnológicos o cualquier otro medio**, tomando en cuenta su edad y condición. [el destacado es nuestro]

Por su parte, el artículo 494 ter del Código Penal sanciona el delito de "acoso sexual", referido en su numeral segundo a lo que se denomina *stalking* en el derecho extranjero, en los siguientes términos:

> Art. 494 ter. Comete **acoso sexual** el que realizare, en lugares públicos o de libre acceso público, y sin mediar el consentimiento de la víctima, un acto de significación sexual capaz de provocar una situación objetivamente intimidatoria, hostil o humillante, y que no constituya una falta o delito al que se imponga una pena más grave, que consistiere en:
>
> 1. Actos de carácter verbal o ejecutados por medio de gestos. En este caso se impondrá una multa de una a tres unidades tributarias mensuales.
>
> 2. Conductas consistentes en **acercamientos o persecuciones**, o actos de exhibicionismo obsceno o de contenido sexual explícito. En cualquiera de estos casos se impondrá la pena de prisión en su grado medio a máximo y multa de cinco a diez unidades tributarias mensuales. [el destacado es nuestro]

No obstante esta norma no hace referencia expresa a actos de acoso a través de medios tecnológicos, otra figura penal, llamada "acoso sexual en espacios públicos", del artículo 161-C del Código Penal, sí dispone la posibilidad de cometer el delito señalado, sea usando estos (u otros medios) para obtener el contenido o bien para difundirlo.

> Art. 161-C. Se castigará con la pena de presidio menor en su grado mínimo y multa de cinco a diez unidades tributarias mensuales, al que en lugares públicos o de libre acceso público y que **por cualquier medio capte, grabe, filme o fotografíe imágenes, videos o cualquier registro audiovisual**, de los genitales u otra parte íntima del cuerpo de otra persona con fines de significación sexual y sin su consentimiento.
>
> Se impondrá la misma pena de presidio menor en su grado mínimo y multa de diez a veinte unidades tributarias mensuales, al que **difunda dichas imágenes, videos o registro audiovisual** a que se refiere el inciso anterior.
>
> En caso de ser una misma la persona que los haya obtenido y divulgado, se aplicarán a ésta, la pena de presidio menor en su grado mínimo a medio y multa de veinte a treinta unidades tributarias mensuales. [el destacado es nuestro]

La misma fórmula de comisión del delito de acoso ("por cualquier medio") utilizan la Ley 19.712 de 2001, Ley del Deporte, modificada por Ley 21.197 de 2020, que regula el acoso sexual en el deporte[20], y el Código del Trabajo, que contempla el acoso sexual en el espacio laboral y el acoso laboral propiamente

[20] Art. 40 P numeral 5 letra c), Ley 19.712: **Acoso sexual**: Cualquier conducta en que una persona realice, **por cualquier medio**, requerimientos de carácter sexual no consentidos por quien los recibe y que amenacen o perjudiquen su situación deportiva o sus oportunidades de competición. [el destacado es nuestro]

tal[21]. En cambio, la Ley 21.369 de 2021, que regula el acoso sexual en la educación superior, hace expresa referencia al acoso en el espacio digital, al incluir la conducta sexual cuando es "virtual o telemática".

> Art. 2° inc. 2, Ley 21.369: Constituye **acoso sexual** cualquier acción o conducta de naturaleza o connotación sexual, sea verbal, no verbal, física, presencial, **virtual o telemática**, no deseada o no consentida por la persona que la recibe, que atente contra la dignidad de una persona, la igualdad de derechos, su libertad o integridad física, sexual, psíquica, emocional, o que cree un entorno intimidatorio, hostil o humillante, o que pueda amenazar, perjudicar o incidir en sus oportunidades, condiciones materiales o rendimiento laboral o académico, con independencia de si tal comportamiento o situación es aislado o reiterado. [el destacado es nuestro]

2. El proyecto de ley que prohíbe conductas de violencia digital (boletín N° 13.928-07)

El proyecto de ley que proscribe, tipifica y sanciona la violencia digital en sus diversas formas y otorga protección a las víctimas de la misma, boletín N° 13.928-07, está siendo revisado en primer trámite constitucional en la Comisión de Seguridad Ciudadana de la Cámara de Diputadas y Diputados.

El señalado proyecto de ley aborda la violencia digital en general y hacia las mujeres en particular, a partir de la penalización de las mismas y, como señala el mismo proyecto, para "que el Estado adopte la obligación, mediante las multas obtenidas por los delitos aquí sugeridos, de prevenir a través de la educación digital, resocializar a victimarios de modo de evitar que vuelvan a cometer vulneraciones de este tipo, además de generar programas de reparación para las víctimas de los mismos".

a. Definición de violencia digital

El artículo 2° de proyecto de ley define la violencia digital de la siguiente manera:

> Artículo 2º.- De la violencia digital. Será constitutivo de violencia digital **todo acto realizado a través de medios, plataformas o dispositivos tecnológicos** y que atente contra la integridad, la dignidad, la intimidad, la libertad, la vida privada o cause daño o sufrimiento psicológico, físico, económico, sexual o a la identidad o expresión de género tanto en el ámbito privado como en el público; incluyendo el daño moral que estos hubieran provocado. [el destacado es nuestro]

[21] Art. 2 inc. 2, Código del Trabajo: Las relaciones laborales deberán siempre fundarse en un trato compatible con la dignidad de la persona. Es contrario a ella, entre otras conductas, el **acoso sexual**, entendiéndose por tal el que una persona realice en forma indebida, **por cualquier medio**, requerimientos de carácter sexual, no consentidos por quien los recibe y que amenacen o perjudiquen su situación laboral o sus oportunidades en el empleo. Asimismo, es contrario a la dignidad de la persona el **acoso laboral**, entendiéndose por tal toda conducta que constituya agresión u hostigamiento reiterados, ejercida por el empleador o por uno o más trabajadores, en contra de otro u otros trabajadores, **por cualquier medio**, y que tenga como resultado para el o los afectados su menoscabo, maltrato o humillación, o bien que amenace o perjudique su situación laboral o sus oportunidades en el empleo. [el destacado es nuestro]

Esta disposición, a diferencia de otras conductas (contenidas en los artículos 4 a 8), no establece una sanción específica, sino que define para efectos pénales la violencia digital, contemplando la conducta, medio de comisión y el objeto del delito.

Luego, el inciso segundo enumera las conductas a través de las cuales se manifiesta la violencia digital:

- Acoso, acecho, monitoreo u hostigamiento de personas;
- Difusión no consentida de contenido íntimo y la explotación sexual facilitada por la tecnología;
- Comunicación ilícita de datos personales de otro;
- Suplantación de identidad o manipulación de información;
- Coacción y amenazas;
- Lenguajes de odio y discriminación;
- Desprestigio y difusión de información falsa, y
- Actos que socavan el libre desenvolvimiento de la personalidad en el espacio digital.

Sin embargo, se observa que el proyecto de ley solo prohíbe y penaliza algunas de las conductas enumeradas, al reiterarlas y subsumirlas en los tipos penales de los artículos 4 a 8, dejando otras sin sancionar (como la coacción y amenazas o la explotación sexual).

b. Conductas punibles (tipos penales)

Revisadas las normas, se observa que las descripciones de los tipos penales de los artículos 4 a 8 del proyecto de ley no cuentan con un criterio común, en cuanto delitos en el contexto de lo que el mismo proyecto define como violencia digital, como se verá a continuación.

i. Exhibición o difusión de datos personales (*doxing*)

De acuerdo a su redacción, esta conducta ilícita requiere, como medio de comisión del delito, “cualquier medio apto para su difusión pública”, sin que necesariamente se trate de un medio digital o tecnológico.

> Art. 4. Comunicación ilícita de datos personales. Quien, de forma deliberada e ilegítima, comunique públicamente o exhiba **por cualquier medio apto para su difusión pública** el teléfono personal de otro, su correo electrónico o datos que permitan ubicarlo físicamente será castigado con multa de veintiuna a treinta unidades tributarias mensuales.
>
> Están exentos de responsabilidad penal por las conductas sancionadas en este artículo quienes publiquen información por razones de interés público. [el destacado es nuestro]

ii. Suplantación de identidad por medios digitales

En este caso el medio de comisión del delito está enunciado en el encabezado del artículo pero no en la descripción de la conducta, por lo que no sería parte del tipo penal.

> Art. 5. Suplantación de identidad **por medios digitales**. Quien realice una suplantación no consentida y convincente de la identidad de otra persona, con el fin de generar una situación intimidatoria, hostil o humillante, será castigada con pena de multa de veintiuna a treinta unidades tributarias mensuales.
>
> Quien realice la conducta descrita en el inciso anterior con el fin de obtener que otra persona le envíe contenido indicado en el artículo ocho de esta ley, será castigado con multa de treintaiuna a cincuenta unidades tributarias mensuales. [el destacado es nuestro]

iii. Envío o exhibición de contenido no solicitado (*cyberflashing*)

Aquí se observa una total ausencia del medio de comisión del delito en el espacio digital y, por tanto, no se trataría de una conducta que configure violencia digital.

> Art. 6. Envío o exhibición de contenido no solicitado. Quien realice un envío o una exhibición de material no solicitado, cuyo contenido es violento, de desnudo total o parcial, con connotación sexual o sexualmente explícito, y que provoque una situación intimidatoria, hostil o humillante será castigado con once a veinte unidades tributarias mensuales.

iv. Acoso digital (*cyberstalking*)

Aunque la norma propuesta utiliza los verbos rectores “se comunique” o “intentare comunicarse”, este tipo penal podría comprender comunicaciones convencionales y no necesariamente digitales. A modo de ejemplo, tal como se reseñó anteriormente, la legislación del estado de California se refiere a “un medio de comunicación electrónica” y a continuación entrega una lista abierta de casos (teléfonos, teléfonos celulares, computadoras, grabadoras de video, máquinas de fax, buscapersonas, asistentes digitales personales, teléfonos inteligentes y cualquier otro dispositivo que transfiera signos, señales, escritura, imágenes, sonidos o datos).

Además, sin perjuicio de que las acciones típicas del denominado *cyberstalking*, como son acechar, monitorear y hostigar se encuentran entre las las conductas a través de las cuales se puede manifestar la violencia digital (como señala el art. 2 inc. 2 del proyecto de ley), ellas no están consideradas como verbos rectores para la comisión del tipo penal en comento.

> Art. 7. Acoso digital. El que de cualquier forma y sin consentimiento de otra persona, afectando las condiciones de su vida privada, reiteradamente **se comunique o intentare comunicarse** con ella será castigado con multa de once a veinte unidades tributarias mensuales.
>
> Si la comunicación involucrase la revelación de datos que permitan ubicar físicamente a la víctima, o el envío del contenido indicado en el artículo ocho de esta ley del que la víctima sea titular, no deberá ser reiterada para que constituya acoso y será sancionado con multa de veintiún a treinta

> unidades tributarias mensuales, excepto que hubiera un delito con una pena más grave. [el destacado es nuestro]

v. Difusión no consentida de contenido íntimo

En esta materia se observa que algunas conductas de ciberacoso, consideradas por la legislación extranjera, no fueron incluidas en el proyecto de ley en comento, como la instalación de software de monitoreo electrónico o la creación o mantención de sitios web destinados a amenazar a la víctima del acoso (estado de Illinois, EE.UU.).

> Art. 8. Difusión no consentida de contenido íntimo. Al que, habiendo obtenido una imagen, registro audiovisual, real o simulado, de desnudo total o parcial, con connotación sexual o sexualmente explícito, le diere **difusión por cualquier medio** sin haber requerido y obtenido previamente el consentimiento de la víctima, será castigado con multa de doscientas cincuenta a quinientas unidades tributarias mensuales.
>
> Cuando para materializar el hecho lo realice **mediante comunicación pública o por cualquier medio apto para su difusión pública**, será castigado con multa de cuatrocientas a seiscientas unidades tributarias mensuales. [el destacado es nuestro]

a) Agravantes

De acuerdo al artículo 9 propuesto, serían circunstancias agravantes de las conductas sancionadas en esta ley:

- Realizar el delito con ánimo de lucro.
- Cometer el delito por quien fuere, o hubiere sido cónyuge o conviviente de la víctima, o por quien mantuviere o hubiese mantenido con ella una relación de carácter sexual o sentimental sin convivencia.
- Cometer el delito por parte del padre o madre de un hijo común con la víctima.
- Mantener una relación laboral, académica o profesional con la víctima.
- Realizarlo por quien fuere mayor de edad en contra de quien no lo sea.
- Cometer el delito o participar en el motivado por la ideología, opinión o afiliación política, religión o creencias de la víctima; la nación, raza, etnia o grupo social a que pertenezca; su sexo, orientación sexual, identidad de género, edad, filiación, apariencia personal o la enfermedad o discapacidad que padezca.

No fueron incluidas en este listado otras posibles agravantes observadas en el derecho comparado, como haber obtenido el contenido difundido de la víctima estando ésta en estado de ebriedad o bajo el influjo de drogas.

Fuentes jurídicas

- **Australia**

Criminal Code Act 1995. Disponible en: http://www.ejustice.just.fgov.be/eli/loi/2005/06/13/2005011238/justel#LNK0073 (abril, 2022).

- **Chile**

Código Penal. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1984&idParte=&idVersion= (abril, 2022).

Ley 19.712 de 2001, Ley del Deporte. Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=181636&idVersion=2021-10-23&idParte= (abril, 2022).

Ley General de Educación (DFL 2 fija texto refundido, coordinado y sistematizado de la Ley Nº 20.370 con las normas no derogadas del Decreto con Fuerza de Ley Nº 1, de 2005). Disponible en: https://www.bcn.cl/leychile/navegar?idNorma=1014974&idParte=0&idVersion= (abril, 2022).

Proyecto de ley que proscribe, tipifica y sanciona la violencia digital en sus diversas formas y otorga protección a las víctimas de la misma, boletín N° 13.928-07. Disponible en: https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=14490&prmBOLETIN=13928-07 (abril, 2022).

- **España**

Código Penal. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444 (abril, 2022).

- **Estados Unidos**

US Code. Disponible en: https://www.law.cornell.edu/uscode/text (abril, 2022).

Illinois Statutes Chapter 720. Criminal Offenses §-7.5.Cyberstalking. Disponible en: https://codes.findlaw.com/il/chapter-720-criminal-offenses/il-st-sect-720-5-12-7-5.html

California Penal Code. Disponible en: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=15.&part=1.&chapter=2.&article= (abril, 2022).

- **México**

Ley General de Acceso de las Mujeres a una Vida Libre de Violencia. Disponible en: http://www.ordenjuridico.gob.mx/Documentos/Federal/pdf/wo17079.pdf (abril, 2022).

Código Penal del Estado de México. Disponible en: http://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/cod/vig/codvig006.pdf (abril, 2022).

Referencias

Council of Europe (2018). Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018. Cybercrime Convention Committee (T-CY) Working Group on cyberbullying and other forms of online violence, especially against women and children. Disponible en: https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914 (abril, 2022).

European Parliament Research Service (2018). Victims of cyberbullying [What Europe does for you]. Disponible en: https://epthinktank.eu/2018/10/28/victims-of-cyberbullying-what-europe-does-for-you/ (abril, 2022).

Segegob (2021). #InfluenciaLoBueno: Gobierno lanza campaña contra el ciberacoso y llama a fomentar el buen trato en redes sociales. Disponible en: https://msgg.gob.cl/wp/2021/12/24/influencialobueno-gobierno-lanza-campana-contra-el-ciberacoso-y-llama-a-fomentar-el-buen-trato-en-redes-sociales/ (abril, 2022).

Stopbullying.gov (2021). What Is Cyberbullying. Disponible en: https://www.stopbullying.gov/cyberbullying/what-is-it (abril, 2022).