LUIS MIGUEL RUSSI PULGAR

CONCEPTO, TIPOLOGÍA Y ETIOLOGÍA DEL ACOSO MORAL COMO CIBERCRIMEN AUTÓNOMO-SOCIAL EN EL DERECHO PENAL

(Tesis de Grado de Maestría)

BOGOTÁ D.C., COLOMBIA

2019

“Por lo demás, el problema central es irresoluble: la enumeración, siquiera parcial, de un conjunto infinito. En ese instante gigantesco, he visto millones de actos deleitables o atroces; ninguno me asombró como el hecho de que todos ocuparan el mismo punto, sin superposición y sin trasparencia.”

(J.L. Borges, *El Aleph*, 1945)

“Esa obra era un escándalo, porque la confusión y la maravilla son operaciones propias de Dios y no de los hombres.”

(J.L. Borges, *Los Dos Reyes y los Dos Laberintos*, 1939)

“We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology”

(Carl Sagan, 2006).

CONTENIDO

Introducción. El Acoso en la Cuarta Revolución Humana

El tópico del acoso y del hostigamiento —y por esta vía, del ciberacoso y del ciberhostigamiento— en el ordenamiento jurídico colombiano ha sido disperso y poco relevante. Lo anterior se evidencia a partir de un análisis de las políticas públicas (incluida la política criminal) que buscan combatir este tipo de comportamientos.

En efecto, el cambio de mentalidad constitucional de 1991, el cual supuso importantes cambios en un sinnúmero de ámbitos de la vida nacional (por ejemplo, los derechos fundamentales, la acción de tutela, la descentralización territorial, entre otros), no trajo ninguna reforma relevante frente a este tema. Tal vez la única consideración tangencial sobre ello sea la consignación del reconocimiento del asilo político en el artículo 36 de la Carta, lo que supone un reconocimiento implícito del acoso político. En efecto, el asilo político o territorial ha sido definido como "una garantía que tiene toda persona ante el ordenamiento jurídico internacional, y significa la expresión humanitaria debida a la racionalidad. El asilo surge como una medida que remedia el estado de indefensión de una persona frente a un sistema del cual es disidente, por motivos de opinión política o religiosa. (…) el asilo, se repite, trata de evitar el estado de indefensión individual ante una amenaza estatal contra una persona, por motivos de índole política, filosófica, religiosa o doctrinaria."[1] En este sentido, es posible intuir que el fundamento de la figura del asilo político consagrada en la Carta de 1991 es la solidaridad internacional frente a los sujetos que política, filosófica, religiosa o doctrinalmente son acosados por sus visiones y opiniones en su país de origen, o en el que residan.

Más allá de ello, en el nivel legislativo, los códigos penales de 1936, 1980 y 2000, no sancionaban ninguna conducta de acoso —ni mucho menos de ciberacoso— , lo cual es llamativo para el caso de la codificación de 2000, promulgada en el cambio de milenio, cuando el auge y consecuencias del Internet comercial ya estaban en su apogeo a partir de un drástico crecimiento de su uso en los años 90.

Solo hasta el año 2006, en el ámbito del derecho laboral, se reconoció como lesiva la conducta del acoso (laboral) mediante la expedición de la Ley 1010 de 2006. Empero, si bien las denuncias sobre dicha conducta han venido en aumento, son pocos los casos que se resuelven a favor de las víctimas[2].

---

[1] Corte Constitucional. Sentencia C-186 de 1996, M.P.: Vladimiro Naranjo Mesa.

[2] Según cifras del Ministerio del Trabajo, en el año 2018, hasta el mes de agosto, se habían denunciado 1.406 casos de acoso laboral, de los cuales menos del 10% fue resuelto a favor del denunciante. En todo caso, no debe perderse de vista la alta cifra oscura que envuelven estos casos, en cuanto que las víctimas, por miedo

El acoso sexual solo fue reconocido por el ordenamiento colombiano en el año 2008, con la expedición de la Ley 1257 de ese año, cuyo objeto fue la adopción de normas que permitieran garantizar para todas las mujeres una vida libre de violencia, tanto en el ámbito público como en el privado[3].

En relación con el hostigamiento, la política pública-criminal ha sido aún más dispersa, al desligar este comportamiento de la conducta de acoso y al limitarla a unos determinados grupos sociales, en una equiparación no explícita con las regulaciones sobre discurso del odio. Fue así como en el año 2011 se consagró en el artículo 134B del Código Penal la conducta de hostigamiento (Ley 1482 de 2011, posteriormente objeto de reforma mediante la Ley 1752 de 2015), como un tipo penal lesivo del bien jurídico vida e integridad personal, lo cual no ha estado exento de críticas[4].

El acoso escolar tampoco es una conducta punible, ni siquiera cuando es cometida por un estudiante mayor de edad en el ámbito escolar o por un miembro del cuerpo educativo escolar, y solo se tornó relevante en el debate nacional cuando el estudiante Sergio Urrego decidió quitarse la vida, saltando desde un piso elevado de un centro comercial en la ciudad de Bogotá, después de haber sido acosado y hostigado por las directivas del colegio donde estudiaba por su condición de homosexual.

El acoso inmobiliario no ha sido objeto de legislación o mayor comentario doctrinal en Colombia.

En este sentido, se vislumbra como el legislador no ha sido consistente y comprehensivo de las conductas de acoso u hostigamiento, circunscribiéndolas a determinados condicionamientos (la búsqueda de favores sexuales o la motivación discriminadora). Si bien dichas orientaciones tienen fundamento en fines nobles devenidos de los estudios de género o de la lucha contra la discriminación, lo cierto es que un tratamiento integral se hace imperativo, con el fin no solo de salvaguardar una mayor precisión teórica y dogmática que repercuta en beneficio del principio de legalidad y de tipicidad, sino también en beneficio de la protección de las víctimas.

---

a perder su trabajo (entre otras razones), prefieren no denunciar. [https://www.portafolio.co/economia/empleo/el-acoso-laboral-crece-en-colombia-520447]

[3] Según cifras de la Fiscalía General de la Nación, en 2018 se radicaron 543 denuncias por el delito de acoso sexual, lográndose la comparecencia del presunto agresor ante un juez de la República solo en 22 casos de ese total. A febrero de 2019, 119 de esas denuncias seguían en etapa de indagación y 393 fueron archivadas por ser considerados los hechos como de menor gravedad. Como en el acoso laboral, la cifra oscura en este tema también es alta. [https://www.elespectador.com/noticias/bogota/ejemplar-condenan-12-anos-de-carcel-acosador-en-transmilenio-articulo-839786]

[4] POSADA MAYA, Ricardo. *Delitos contra la vida y la integridad personal*, T. II, Bogotá, Ibáñez, Universidad de los Andes, 2015, pp. 191 y ss.

Tal vez la desidia de la legislación colombiana se deba a razones de naturaleza extralegal, más cercana a conceptos culturales y por ello también políticos, consistente en considerar el problema del acoso y del hostigamiento como situaciones problemáticas exclusivas del primer mundo o de los países industrialmente desarrollados. En este sentido, parte de la doctrina más difundida y respetada del país ha sido consistente en señalar la tipificación de estas conductas (hostigamiento y acoso sexual) como meras manifestaciones simbólicas del derecho penal que se traducen en una vil expansión en detrimento de las garantías fundamentales.

Sin embargo, esa idea de que en Colombia el acoso y el hostigamiento no son problemas sociales reales o que hacen parte de una idiosincrasia cultural no lesiva, está lejos de ser verdad, como lo han demostrado los diversos informes que han analizado las consecuencias de este tipo de conductas en sectores poblacionales vulnerables, como son los jóvenes, los homosexuales o las mujeres. En nuestro entender, adoptar semejante visión sobre esta problemática y comportamientos desviados es querer pensar que el país está y estará siempre anclado en un subdesarrollo económico del siglo XIX, cuando la realidad es otra. Si bien Colombia no es una potencia mundial, sí es un país industrializado[5], que hace parte del concierto internacional y que como sociedad moderna que es, replica muchos de los problemas sociales que en este tipo de sociedades se presentan, como es el abuso en contra de las personas mediante las nuevas tecnologías de la información y la comunicación (TIC).

Así, los efectos nocivos del vertiginoso desarrollo tecnológico que ha vivido la humanidad en los últimos 60 años, en especial a partir de la década de los 60 (cuando nace el primer trabajo comunicativo mediante una red —*networking*— en el Instituto Tecnológico de Massachusetts —MIT, por sus siglas en inglés—) no han sido ajenos en el territorio colombiano, como no lo pueden ser por el simple hecho de ser los colombianos parte de la especie humana, la cual ha dominado el "arte" tecnológico.

La importancia de los efectos de las TIC en nuestras sociedades es gráficamente explicada por Yuval Noah Harari, un profesor de historia de la Universidad de Jerusalén, quien, a principios de la década, en el año 2011, publicó una breve historia de la humanidad (un ensayo histórico de fácil digestión para el público lector masivo) titulado *From animals into Gods*[6]. En dicho ensayo, Harari señala que la historia de la humanidad puede dividirse en tres eventos o revoluciones

[5] OCAMPO GAVIRIA, José Antonio, *et ál*. "La industrialización y el intervencionismo estatal (1945-1980)", en OCAMPO GAVIRIA, José Antonio. *Historia económica de Colombia*, Bogotá, Fedesarrollo, 2007, pp. 271 y ss.
[6] HARARI, Yuval Noah. *From Animals into Gods*, Scotts Valley, Create Space, 2012, *passim*. En español, ÍD. *De animales a dioses*, Barcelona, Penguin Random House, 2014.

claves que soportaron a la especie humana para catapultarse en el dominio global sobre las demás especies con las que comparte el planeta.

En un primer lugar, hace aproximadamente 220 mil años, los humanos desarrollaron el lenguaje para poder comunicarse entre sí y lograr la colaboración necesaria para construir sociedad y aventajar a las demás especies a través de la ayuda mutua que aún hoy nos préstamos. Este momento es denominado como la Revolución Cognitiva (o del lenguaje).

En segundo lugar, hace 20 mil años, los humanos trocaron su actividad nómada para empezar a asentarse en territorios fértiles, con el objeto de trabajar la tierra y subsistir de ella, de tal forma que grandes poblaciones empezaron a conformarse alrededor de la actividad agrícola. Con ello, fue posible alimentar a la especie humana, que cada día crecía y se reproducía exponencialmente. Este momento fue identificado como la Revolución Agrícola.

Finalmente, hace algo más de 500 años, el hombre adoptó, a través de sendos ejercicios filosóficos previos, el método del discurso racional, o lo que es lo mismo, el método científico. El objetivo (presente desde los antiguos) era contestar las grandes preguntas de la humanidad, solo que esta vez sometiendo el tema de estudio (el objeto epistemológico) a las estrictas reglas de las ciencias naturales. Este momento, cuando el hombre se dio cuenta de su insignificancia en el universo, se le identificó como la Revolución Científica.

Así, con base en estos tres hitos, la humanidad llegó hasta este siglo XXI como absoluto dueño y amo del planeta que habita. Empero, contrario a lo señalado por FUKUYAMA en su clásico ensayo sobre el fin de la humanidad publicado en el cambio de milenio[7], todavía le restan demasiados retos a nuestra especie sobre la Tierra. Tal vez uno de los más apremiantes es el relacionado con el desarrollo de las nuevas tecnologías digitales, informáticas y de la comunicación en general. Internet, y todas sus posibilidades, ha penetrado de tal forma nuestras vidas que hoy es imposible pensar en la cotidianeidad sin reflexionar en las implicaciones de *WhatsApp*, Facebook o las páginas web en nuestras vidas.

Las consecuencias de las nuevas tecnologías en las sociedades y en las personas cumplen con las premisas del principio de doble efecto, en cuanto que ellas han generado no solo grandes avances positivos en múltiples campos (la medicina, el deporte, el entretenimiento, la seguridad, el comercio, etcétera), sino que a su vez también han afectado de forma negativa el funcionamiento social (por ejemplo, el

[7] *Vid.* FUKUYAMA, Francis. *The End of History and the Last Man*, New York, The Free Press, 1992.

funcionamiento democrático de las sociedades a través de la manipulación de los electores[8]) o algunos bienes valorados por los individuos, como su intimidad o su salud mental[9].

Por ello, no es un desatino afirmar, como lo hace Harari en la secuela de su breve historia de la humanidad (denominada por él una "breve historia del mañana"), que estamos en el medio de una cuarta revolución igual de trascendental como las anotadas en su ensayo: la Revolución Tecnológica.

Considerando lo incipiente de la nueva vida tecnológica, hoy no tenemos certezas sobre las múltiples consecuencias que esta revolución tendrá en nuestras vidas. ¿Cómo se comportará el derecho cuando los robots sean una realidad? ¿Qué juicios de reproche hará el derecho penal cuando las decisiones sean tomadas por un algoritmo autónomo? ¿Qué política de creación de contenidos adoptará el Estado colombiano cuando se masifique la creación de códigos libres y abiertos en Internet? ¿Qué estamos haciendo para reducir las complejidades de un territorio desubicado y neutro como es la Red?

No obstante, las reflexiones sobre estos temas desde las ciencias jurídicas —por lo menos parcialmente—, en Colombia, ya existen. En concreto, a partir de la Ley 1273 de 2009 y de sendos documentos estatales (Conpes, resoluciones, decretos, etc.) Colombia ha venido adoptando sendas políticas públicas y también políticas criminales para acometer las diversas situaciones, positivas o negativas, que surgen del desarrollo cibertecnológico. Así, se ha propendido por la ampliación de cobertura tecnológica en los territorios y se han dispuesto la implementación de un verdadero "Gobierno en Línea". A su vez, en el ámbito jurídico-penal, se ha tendido hacia la criminalización de actos abusivos en contra de la información y los datos a través del uso de las nuevas tecnologías, llegándose a sustentar una nueva categorización criminal: la criminalidad informática.

Infortunadamente, los anteriores esfuerzos, si bien han sido amplios y decisivos, en muchos campos se han quedado cortos, en especial en la dimensión personal de los antiguos o clásicos bienes jurídicos, ya que ha existido un afán legislativo

---

[8] En octubre de 2019, Mark Zuckerberg fue citado por segunda vez al Congreso de los Estados Unidos para rendir cuentas sobre las malas prácticas de Facebook en relación con la diseminación de información falsa en esa red social con el fin de manipular a los electores [https://www.elespectador.com/opinion/editorial/la-endeble-defensa-de-mark-zuckerberg-articulo-890162.]

[9] Cfr. NAVARRO RODRÍGUEZ, Miguel; BARRAZA MACÍAS, Arturo. "Redes sociales y uso patológico del Internet: síntomas y efectos negativos en jóvenes", en *XI Congreso Nacional de Investigación Educativa* [*vid.* en http://www.comie.org.mx/congreso/memoriaelectronica/v11/docs/area_07/0295.pdf]

por sancionar las novísimas conductas de cibercriminalidad (teorizando nuevos conceptos de acción, resultado, nexo de causalidad, bien jurídico, *et ál*), pero sin prestar demasiada atención a viejas conductas que se ven hiperamplificadas en sus efectos nocivos a través del uso criminal de las nuevas tecnologías. En efecto, como se expondrá en este trabajo, existen viejas conductas que, al hacerse valer de las nuevas tecnologías, crean una serie de nuevos riesgos lesivos de bienes jurídicos clásicos, como la libertad o la autonomía. Este es el caso del ciberacoso.

En esta materia, el legislador se ha conformado por considerar, desde la parte general del Código Penal, dichas situaciones como una circunstancia de mayor punibilidad (numeral 17 del artículo 58 de la Ley 599 de 2000, adicionado por el artículo 2 de la Ley 1273 de 2009), no valorando la necesidad de proteger sendos bienes jurídicos (dado el carácter pluriofensivo de estas conductas) de forma autónoma. El ciberacoso y el ciberhostigamiento son típicos ejemplos de ello, en cuanto que no existen en nuestra legislación como conductas independientes y la solución que brinda el ordenamiento jurídico en situaciones en que se presentan esas conductas es la de considerar que, al existir la intervención de las TIC, deba tenerse la circunstancia como una de mayor punibilidad en el marco del juzgamiento de un delito cercano, como sería el constreñimiento ilegal o un delito de amenazas. Cuando no sea posible adecuar los hechos a esos delitos cercanos, la solución que provee el ordenamiento es la impunidad.

En este sentido, el presente trabajo busca acometer un análisis criminológico y jurídico de una de las nuevas formas de ciberdelincuencia que con mayor auge se viene desarrollando en Colombia y el mundo[10], como son el ciberacoso (*cyberstalking*) y el ciberhostigamiento (*cyberharassment*) mediante las nuevas tecnologías de la comunicación y la información.

Puesto que en nuestro ordenamiento jurídico no existe un reconocimiento expreso de estas conductas como típicas (más allá de las consignadas en los artículos 134B y 210A de la Ley 599 de 2000, cuyas características y diferencias serán analizadas), se hace menester, de cara a la sociedad colombiana, determinar el carácter lesivo y desviado de dichos actos mediante su conceptualización.

Existe sin duda una falta de claridad sobre lo que debe entenderse por acoso y por ciberacoso, y por hostigamiento y ciberhostigamiento; se discute si estos conceptos son diferentes o son iguales, si uno se comporta como extensión del otro o si simplemente estamos frente a conductas idénticas con meras diferencias instrumentales o modales, respecto de la forma en que se ejecutan.

[10] Algunos datos de la prevalencia del problema serán suministrados en el capítulo pertinente.

Para poder dilucidar dicho tema se hace necesario adoptar un concepto de criminalidad informática o de criminalidad cibernética que permita abarcar y excluir las conductas que en realidad han evolucionado a partir de la Revolución Tecnológica de aquellas otras que solo están adaptándose a nuevas formas comisivas sin modificar la naturaleza de sus injustos penales.

Tenemos para nosotros que los análisis realizados sobre este tópico conceptual han incurrido en dos grandes errores: de un lado, se ha querido sostener un concepto de delincuencia relacionado con las TIC sometido a una pureza aparente que excluya a las viejas conductas y a los viejos bienes jurídicos; mientras que del otro lado, no se ha prestado suficiente atención a la influencia de la Revolución Tecnológica en las conductas de acoso y de hostigamiento para poder fundamentar conceptos mixtos o puros de acoso y hostigamiento cibernético.

Así, contrario a ello, tomando en serio las repercusiones del Internet, el ciberespacio, las TIC y en general de la Revolución Tecnológica, llegamos a sostener que el acoso cibernético, a partir del especial hábitat en el cual se desarrollan las nuevas relaciones sociales cibernéticas, es un verdadero cibercrimen cuyo injusto disvalioso requiere de formas concretas de gestión y prevención, y el cual se diferencia de un acoso físico o predatorio clásico cuya conexión con las TIC es meramente instrumental.

La preeminencia del conflicto que se genera por parte de la conducta ciberacosadora es uno de gran relevancia contemporánea, pues a la par del desarrollo tecnológico, se irá paralelamente acentuando la conducta desviada, encontrando nuevos espacios (o mejor: ciberespacios) de manifestación, y así, nuevas formas de victimización.

Las cuestiones jurídicas que a partir de este análisis se desprendan, serán muchas y variadas, relacionadas con la teoría del bien jurídico, la teoría del delito, los resultados jurídicos o naturales exigidos, la dimensión espacial de la ley penal, la teoría del proceso, la prueba, la teoría de la pena, entre otras, que ameritan trabajos autónomos, empero su comentario en este trabajo servirá para visualizar las aristas del problema social y comunitario que se estudia y las repercusiones que su falta de tratamiento por parte de la ley penal tiene frente a la cibercomunidad.

Así, en conclusión, el objeto de este trabajo es otorgarle autonomía conceptual a un fenómeno que ha sido mezclado en el derecho comparado y vernáculo con otros de igual importancia y necesidad de gestión, pero cuyo acometimiento será imposible si no se parten de las bases conceptuales precisas que permitan diferenciar entre la persecución acosadora y la degradación hostigadora, como

puntos de partida de conceptos dependientes o independientes de ciberacoso y ciberhostigamiento.

CAPÍTULO PRIMERO

Concepto, clasificación y características del cibercrimen y cibercriminalidad

I. Ciberespacio, cibercriminalidad y cibercrimen

A. Introducción

Es un lugar común identificar al ciberespacio como sinónimo del Internet. Sin embargo, los dos conceptos son diferentes, comportándose el ciberespacio como uno más amplio que el concepto de Internet, pero en todo caso, interdependientes. Según la Real Academia de la Lengua Española, el ciberespacio es un ámbito virtual creado por medios informáticos[11], mientras que el Internet es una "red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación."[12] En este sentido, el ciberespacio se refiere a un concepto metafísico, referido a un espacio que no existe en el mundo físico, mientras que Internet hace referencia a un concepto instrumental e infraestructural, más físico, que hace posible que las comunicaciones que se desarrollan en el ciberespacio existan[13].

La palabra ciberespacio entró en el argot cultural por vía de la literatura, ya que el primero en acuñarla fue el escritor de ciencia ficción William Gibson en su novela *Neuromante*, publicada en 1984[14]. Por otro lado, el primer ejercicio de comunicación mediante una red (o *networking*) se dio en el Instituto Tecnológico de Massachusetts en 1962, cuando J.C.R. Licklider envió una serie de memos a sus colegas argumentando sobre su concepto de "red galáctica", lo que a la postre sería el Internet[15]. Tras un uso militar y académico, el gobierno de los Estados Unidos decidió lanzar el Internet al público en general, en 1995, con la creación del servicio más popular de esa red de comunicación (el *World Wide Web*), lo que

---

[11] [https://dle.rae.es/?id=98Wdd57].

[12] [https://dle.rae.es/?id=LvskgUG]. "Internet es una *red global de dispositivos informáticos* —computadoras, teléfonos móviles, tabletas, consolas de juego, entre otros— que permite enviar, recibir y transmitir datos e información mediante el uso de un protocolo común de comunicaciones." (SAIN, Gustavo. "Internet, el cibercrimen y la investigación criminal de delitos informáticos", en SAIN, Gustavo, AZZOLIN, Horacio. *Delitos informáticos*, Buenos Aires, Montevideo, B de F, 2017, p. 3).

[13] KREMLING, Janine; SHARP PARKER, Amanda M. *Cyberspace, cybersecurity and cybercrime*, Thousand Oaks, SAGE, 2018, pp. 12-13, definen el ciberespacio como "la red interdependiente de infraestructuras de la tecnología de la información, que incluye el Internet, las redes de telecomunicaciones, los sistemas informáticos, y los procesadores y controladores integrados en industrias críticas. En otras palabras, el ciberespacio se refiere al ambiente virtual en el cual las personas se comunican e interactúan con los otros." Por otra parte, definen al Internet como "un sistema global interconectado de redes computacionales que es establecida para intercambiar varios tipos de información." Finalmente, señalan como un error común asimilar el Internet con el *Word Wide Web*: "Mientras que el Internet se refiere a la infraestructura de *hardware* y *software* que conecta computadores alrededor del globo, la *World Wide Web* se refiere a un servicio al que se puede acceder vía el Internet." *(Traducción Libre del Autor, en adelante "Trad. del Aut.")*.

[14] ARBELÁEZ GIRALDO, Andrea. "El ciberespacio y el problema de la realidad virtual", en *Revista de filosofía UIS*, Vol. 16, Bucaramanga, Universidad Industrial de Santander, julio-diciembre de 2017, p. 175.

[15] LEINER, Barry M. *et ál*. *A brief history of Internet*, Internet Society, 1997, p. 3, Accesible en: [https://www.internetsociety.org/internet/history-internet/brief-history-internet/].

en términos económicos significaría un gran desarrollo para las sociedades, al establecerse, en una primera generación del uso de estas tecnologías, una nueva modalidad de negocios: el comercio electrónico[16].

Es a partir de estos hitos fundacionales que se incrusta en la cultura mundial y posteriormente en la cotidianeidad social el uso de las tecnologías de la información y la comunicación, dando paso a nuevos paradigmas sociales que permitieron nuevos alcances para la especie humana, sumergiéndonos de lleno en lo que indicamos como una verdadera Revolución Tecnológica[17]. Los efectos de dicho desarrollo en las personas y en la comunidad han sido tan hondos que han cambiado de forma radical la manera en que interactuamos entre nosotros e incluso la forma en que vivimos. Así, agendar citas con el médico, realizar compras *online*, pagar impuestos mediante una página web o realizar actividades de ocio desde la sala de nuestros domicilios con contrapartes que se encuentran en el otro lado del globo, son solo algunos ejemplos de la forma como la vida individual y comunitaria simplemente no es igual desde el advenimiento del Internet, el acceso libre al ciberespacio y a las nuevas TIC.

Empero, cada paso de la humanidad también es un paso para el crimen, en lo que sería una prueba indiscutible de la máxima que reza que "el delito siempre sigue a la oportunidad". Ilustrativo fue el caso del automóvil, como lo demuestra un pronunciamiento de la Corte Suprema de Justicia de Estados Unidos en 1925:

> "Es sabido por todos los hombres que el cambio radical en el transporte de personas y bienes efectuado por la introducción del automóvil, la velocidad a la cual se mueve, y la facilidad con la cual personas con mentes malignas pueden eludir su captura, ha animado e incrementado grandemente los delitos."[18]

Así, lo dicho para el automóvil también se puede predicar para esta nueva era informática y digital. Nuestra dependencia diaria en las TIC y en el Internet se ha mostrado como una oportunidad idónea para los criminales, quienes han desarrollado a la par de las nuevas tecnologías, también nuevas conductas lesivas necesarias de atención por parte del derecho penal[19]. De ahí que se confeccionara

---

[16] SAIN. "Internet, el cibercrimen y la investigación criminal de delitos informáticos", *cit.,* p. 3.

[17] Algunos la denominan como la "segunda revolución industrial". (SUÁREZ SÁNCHEZ, Alberto. *Manual de delito informático en Colombia*, Bogotá, Universidad Externado de Colombia, 2016, p. 25).

[18] *Brooks* v. *US*, 267 US 432, 438-9 (1925), citado por CLOUGH, Jonathan. *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010, pp. 3. *(Trad. del Aut.).*

[19] "Correlativo a este beneficio, se han desarrollado nuevas formas de delincuencia. La dependencia de la tecnología informática y la telemática, desafortunadamente, ha originado y elevado la delincuencia relacionada con los sistemas de procesamiento y transferencia automática de datos, con riesgo y amenaza no solo de la seguridad y la economía de la sociedad de un país determinado, sino también de la sociedad mundial, por su carácter trasnacional, pues el uso indebido del ordenador y de la tecnología ha contribuido a la conformación de problemas derivados de la llamada 'sociedad de riesgos' (…)." (SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* p. 27).

una nueva categoría de criminalidad, denominada en nuestro medio a partir de una influencia continental europea como "criminalidad informática", pero también conocida en el ámbito del derecho anglosajón como *cybercriminality* o cibercriminalidad[20].

Si bien en Colombia el interés legislativo por combatir algunas de esas conductas apenas tuvo tratamiento sistemático en el año 2009 mediante la Ley 1273 (existiendo como único antecedente a ello la consagración en el Código Penal de 2000 de los tipos de acceso abusivo a sistema informático protegido con medida de seguridad y de sabotaje), la teorización de una categoría autónoma de criminalidad computacional o relacionada con los computadores surgió desde los mismos inicios de estos desarrollos tecnológicos en la década de los sesenta, cuando se hablaba de sabotaje computacional, manipulación computacional, espionaje computacional o uso indebido de sistemas computacionales[21].

El advenimiento de las siguientes décadas solo complejizaría aún más el problema, en cuanto que la dependencia por la tecnología se iba incrementando, llegando la preocupación a situarse a un nivel en el cual no solo se buscaba evitar fraudes económicos, sino salvaguardar a las comunidades de verdaderos ataques remotos que podrían encuadrarse en el concepto de ciberterrorismo, considerando que dichos ataques podrían dar al traste con complejos sistemas cibernéticos que sustentan determinadas formas de vida cotidiana. Solo piénsese en ataques virtuales que pueden generar la suspensión de la prestación de servicios electrónicos o incluso apagones a gran escala de ciudades o grandes proporciones de países.

Por ello, se acuñan los conceptos criminológicos de cibercrimen y cibercriminalidad[22], los cuales comportan verdadera autonomía científica. En contra de ello, podría señalarse que estos conceptos son solo formas pretensiosas de denominar un fenómeno de criminalidad viejo que se está manifestando

---

[20] Si bien algunos consideran a la criminalidad informática como sinónimo de cibercriminalidad y de ciberdelincuencia (POSADA MAYA, Ricardo. *Los cibercrímenes: un nuevo paradigma de criminalidad*, Bogotá, Ibáñez, Universidad de los Andes, 2017, p. 33), como más adelante fundamentaremos, consideramos que la criminalidad informática es una especie de cibercriminalidad, vinculada a los delitos informáticos.

[21] CLOUGH. *Principles of cybercrime*, *cit.,* pp. 3-4.

[22] Estos términos se comportan como neologismos válidos en el español, los cuales devienen de la composición del prefijo "ciber" (derivado de la palabra inglesa *cyberspace*) y del sufijo "crimen" o "criminalidad" (derivados de las palabras inglesas *crime* y *criminality*). "Según las normas de formación de las palabras en español, a partir del prefijo ciber-, como elemento compositivo de numerosas voces relacionadas con la informática y la realidad virtual, se pueden utilizar como neologismos válidos términos como ciberataque, cibercrimen o cibercriminalidad, siempre que se escriban en una sola palabra y sin guion intermedio." (MIRÓ LLINARES, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012, p. 33, n. 2).

mediante nuevos medios[23]. Después de todo, si se analiza con detenimiento, no hay nada nuevo en que los criminales instrumentalicen las tecnologías para la comisión de hechos lesivos de intereses individuales y sociales. De antaño, por ejemplo, las bandas atracadoras de bancos utilizaban radios de radiofrecuencia para su comunicación y para interceptar las comunicaciones de los agentes del Estado que los perseguían. Sin embargo, este argumento —que señala que no debe haber una nueva categorización criminal en cuanto que el fenómeno no es nuevo— se queda corto en su ponderación del contexto que permiten estos nuevos crímenes. En efecto, para entender la autonomía del cibercrimen y de la cibercriminalidad como fenómenos con profundas consecuencias sociales nunca vistas, es necesario reconocerlos como aspectos constitutivos del profundo cambio social generado por la Revolución Tecnológica, en especial, del amplio proceso político, económico y social de la globalización. "En particular, el proceso de globalización económica, que está siendo facilitado por las nuevas TIC, no solo provee oportunidades rentables de desarrollo internacional de mercados informacionales, sino también simultáneamente eleva el espectro de nuevas actividades criminales que surgen para explotarlos."[24] De esta forma, las mismas tecnologías que nos permiten comunicarnos con otros a miles de kilómetros y que facilitan a los actores del mercado realizar multimillonarios negocios trasnacionales a diario y en segundos, también le ofrecen a las organizaciones criminales novísimas formas de establecer redes globales para la ejecución de sus objetos ilícitos.

> "Las razones son sencillas, la tecnología facilita sustancialmente las relaciones financieras, económicas, comerciales e interpersonales, convirtiéndolas en gestiones de datos eficaces, rápidos y constantes en nuestro medio cultural, como no había sucedido en la historia humana. (…)
>
> En definitiva, la importancia y eficacia del mundo físico comienza a ser igualada e incluso superada por la esfera virtual en muchos aspectos, lo cual significa que los riesgos de las actividades cotidianas pasan del ámbito de competencia de aquellas personas que tienen un dominio físico o analógico de dichas relaciones, a quienes ostentan un dominio efectivo del mundo virtual, valiéndose de medios digitales.
>
> En fin, una cosa es cierta, lo positivo que puedan tener los avances informáticos y telemáticos dentro del contexto de la globalización también involucra aspectos negativos importantes que deben considerarse para optimizar el desenvolvimiento social."[25]

---

[23] Cfr. GRABOSKY, Peter N. "Virtual criminality: old wine in new bottles?", en *Social & Legal Studies*, No. 10:2, Thousand Oaks, SAGE, 2001, pp. 243 y ss.

[24] THOMAS, Douglas; LOADER, Brian D. "Cybercrime: law enforcement, security and surveillance in the information age", en THOMAS, Douglas; LOADER, Brian D. (eds.). *Cybercrime*, Routledge, New York, 2003, p.2. *(Trad. del Aut.)*.

[25] POSADA MAYA. *Los cibercrímenes, cit.,* p. 44.

Efectivamente, el uso de dispositivos informáticos y nuevas tecnologías ha derogado barreras espaciotemporales, ubicándose en el ciberespacio, territorio deslocalizado en el cual no solo suceden negocios o comunicaciones sociales amistosas, sino también delitos de hondas consecuencias económicas, personales y sociales. Como lo reseña SUÁREZ SÁNCHEZ, la informática se muestra como una verdadera nueva forma de poder, ya que quien la usa se coloca en una situación ventajosa frente a los demás[26]. De aquí deviene la creación no solo de nuevos riesgos informáticos, digitales o cibernéticos, sino también la necesidad de configuración de nuevos tipos penales que salvaguarden los intereses relevantes de la concreción de esos riesgos, ya que "hay tantas amenazas como el desarrollo tecnológico lo permita."[27]

B. Conceptualización y clasificación doctrinal

La conceptualización de lo que es un delito informático o un cibercrimen, o de la criminalidad informática, computacional o cibernética, no ha sido pacífica.

1. Así, SUÁREZ SÁNCHEZ reseña que el concepto de delito informático no se ha considerado como una categoría legal, sino criminológica[28], la cual en su inicio era excesiva en su extensión, en cuanto que abarcaba no solo las conductas que lesionaban o ponían en peligro a la información y los datos como bien jurídico autónomo, separable de otros bienes jurídicos individuales, sino también conductas que tuvieran simplemente una conexión directa o indirecta con la informática. Dicho entendimiento era excesivamente amplio, de donde devino la necesidad de acotación y concreción. En este sentido, SUÁREZ SÁNCHEZ adopta el concepto de delito informático como aquella conducta que lesiona la información y los datos, excluyendo de esa compresión conductas tradicionales o nuevas que se valieran de medios informáticos para la lesión de bienes jurídicos tradicionales[29].

---

[26] SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* p. 29.

[27] POSADA MAYA. *Los cibercrímenes, cit.,* p. 47.

[28] De hecho, SUÁREZ SÁNCHEZ (*Manual de delito informático en Colombia, cit.,* p. 54) sostiene que la acotación del sustantivo "delito" dentro de del concepto de "delito informático" bien se podría tener por no afortunada, en cuanto que el concepto de delito bajo la óptica de la teoría del derecho penal tiene un alcance muy limitado, dado que el comportamiento que clasifica para ser delito solo es el que es tipificado de tal manera por la ley penal. "Por tanto, quedarían por fuera de su alcance algunas conductas susceptibles de incriminación vinculadas a la informática que ni aparecen descritas en las normas penales, y que aun siendo sancionables de *lege ferenda* no pueden ser calificadas como delitos."

[29] SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* pp. 55, 57: "Con todo, prefiero la expresión delito informático, entendida como comprensiva de la afectación de la información y los datos como bien jurídico tutelado. (…) Sin embargo, un sector aboga por la reelaboración del concepto de delito informático, para delimitarlo del amplio y genérico delito vinculado con la informática, y elaborar su estructura tipológica teniendo la información en sí misma como interés colectivo y no solo individual, que permita diferenciarlo de cualquier otro ilícito en el cual aparezca vinculada la informática, la

En todo caso, para este doctrinante, el alcance del delito informático no llega solo hasta la protección de la información y los datos, ya que a pesar de ese es el rasgo característico de esta forma de criminalidad, el delito informático es de efectos pluriofensivos y sobre bienes jurídicos intermedios, ya que su tipificación protege bienes jurídicos tradicionales —individuales o colectivos— en conjunción con la tutela que le es propia, relativa a la protección de la información en sí misma, los datos informáticos y la fiabilidad y seguridad colectiva en los medios y sistemas de tratamiento y transferencia de la información[30].

Sobre la criminalidad informática en concreto, SUÁREZ SÁNCHEZ señala que ella se diferencia de otros tipos de criminalidad y comporta autonomía habida cuenta que ostenta unas determinadas características que la alejan de la criminalidad tradicional o clásica, como son (i) la rapidez de su comisión, (ii) la distancia que puede haber entre el lugar de comisión y el lugar de producción del resultado, (iii) la dificultad para descubrir a los autores y la facilidad para borrar huellas y rastros, y (iv) la facilidad para asegurar su impunidad[31].

Así mismo, señala como características básicas criminológicas del delito informático las siguientes[32]:

i. La permanencia y automatismo del hecho, haciendo referencia a la posibilidad de repetición de la acción delictiva, que estimula la permanencia de la comisión del hecho, siendo posible además que una sola acción inicial del agente dé lugar a la repetición del hecho delictivo por un automatismo del sistema.

ii. La gran capacidad de daño, considerando las grandes ganancias que estas conductas generan en el nivel patrimonial y, además, teniendo en cuenta la gran interconexión entre las actividades económicas y sociales que dependen de los sistemas informáticos, generando las conductas efectos en cascada en las que se ven afectadas múltiples personas y entidades.

iii. La facilidad para encubrir el delito, dada la alta complejidad técnica de las conductas, de donde deviene una gran dificultad para probar los

---

telecomunicación, la telemática o la nueva tecnología de procesamiento y trasmisión o transferencia de datos, aunque aquella no resulte directa o indirectamente lesionada. Se aduce que en la actualidad no puede ser definido el delito informático como todo delito vinculado a la informática o a la información, sino como delito del riesgo informático y de la información."

[30] SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* p. 59.

[31] SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* p. 44.

[32] SUÁREZ SÁNCHEZ, Alberto. *La estafa informática,* Bogotá, Ibáñez, UNAB, 2015, pp. 34-37; ÍD. *Manual de delito informático en Colombia, cit.,* pp. 44-47.

hechos punibles, a la par que el especializado conocimiento de los agentes les permite encubrir el hecho y borrar sus huellas, sin mencionar las facilidades que el Internet y el ciberespacio otorgan para permanecer en el anonimato.

iv. La alta cifra negra, que se da en este ámbito por las dificultades de averiguación y comprobación de las conductas, el desconocimiento e ignorancia de las víctimas de que están siendo atacadas o han sido objeto de un ataque y la no denuncia de muchos hechos descubiertos, en especial en el ámbito empresarial, donde no se ponen los hechos en conocimiento de las autoridades para evitar riesgos reputacionales o pérdidas de confianza del público, relacionadas con la vulnerabilidad de sus sistemas informáticos.

v. La ampliación de la criminalidad, en cuanto que cada nuevo desarrollo tecnológico encuentra acomodo en las conductas delictuales.

vi. La separación temporal y el distanciamiento espacial, que implica problemas para la determinación del delito, en cuanto que la acción está muy separada temporalmente del resultado; además del distanciamiento espacial, dado que el sujeto activo puede estar distante de donde se concretan los efectos de su acción ilícita.

vii. Finalmente, el carácter transfronterizo del delito, ya que la posibilidad de que la acción y el resultado se realicen en jurisdicciones totalmente diferentes e, incluso, globalmente distantes, torna a esta criminalidad como desvinculada de los límites territoriales o nacionales.

En conclusión, para SUÁREZ SÁNCHEZ existe una necesidad clara de legislación nueva que pueda acometer los problemas que la era de la información y de la tecnología cibernética ha traído consigo, como lo decidió el legislador colombiano mediante la Ley 1273 de 2009. Con ello, se reconoce la autonomía del nuevo bien jurídico protegido (la información y los datos), sin desconocer que, indirectamente, también se salvaguardan bienes jurídicos tradicionales.

2. Por otra parte, POSADA MAYA realiza una conceptualización de cibercrimen vinculada al delito informático a partir de una clasificación de sus definiciones. En este sentido, señala que existen los delitos informáticos en sentido amplio (o delitos computacionales), de un lado, y delitos informáticos en sentido estricto (o cibercrímenes), del otro, los cuales no deben ser mezclados, agrupados ni

confundidos[33]. Es decir, comparte la misma preocupación de SUÁREZ SÁNCHEZ de que se considere "delito informático" todas las conductas —tradicionales o no— que se vinculen con la informática.

Como fundamento, señala que la doctrina y la jurisprudencia hoy dominantes indican que las fenomenologías cibercriminales son diferentes a los delitos clásicos, no solo porque el objeto material y el bien jurídico son diferentes (la información y los datos), sino por la forma o modo de realización de las conductas, el cual es virtual o informático, a diferencia de los delitos clásicos, en el que es apenas accidental y no consustancial.

> "En consecuencia con lo anterior, se puede afirmar que *los delitos informáticos vinculados a la red (pero que no dependen de la red)*, también llamados delitos computacionales *o informáticos en sentido amplio*, son todas aquellas conductas punibles tradicionales de medios ejecutivos abiertos, que tienen una relación modal objetiva —aunque circunstancial— con el tratamiento de datos e información y los sistemas informáticos (utilización de elementos incorporales). Son delitos que directamente lesionan o ponen en peligro bienes jurídicos como el patrimonio económico, la fe pública, la intimidad personal, la libertad y la formación sexual, el honor, los derechos morales y patrimoniales de autor. Por el contrario, la lesión o puesta en peligro a la seguridad de la información es indirecto y solo tiene explicación a partir del uso del medio empleado: los datos y los sistemas informáticos. Su propósito inicial o principal, pues, no es proteger las funciones informáticas en sentido estricto. (…)
>
> Por el contrario, la doctrina especializada ha dicho que los *cibercrímenes* (o delitos informáticos en sentido *estricto* o *propio*) *son aquellos comportamientos ilícitos que se dirigen a la indebida creación, procesamiento, almacenamiento, adquisición, transmisión, divulgación, daño, falsificación, interceptación, manipulación previa o posterior, y ejecución automática de datos o sistemas informáticos* sin el consentimiento o con abuso del mismo. La finalidad usual de estos comportamientos es lesionar o poner en peligro de manera ilícita (CP art. 11) la seguridad de las funciones informáticas, esto es, la *confiabilidad/confidencialidad* (calidad, pureza, idoneidad y corrección), *integridad*, la *disponibilidad*, el *no repudio* de los datos y los sistemas informáticos protegidos y la *recuperación de información*; sin perjuicio de que esto implique la lesión o la puesta en peligro de otros bienes jurídicos tutelados."[34] (Cursivas del original).

En este orden de ideas, para POSADA MAYA lo fundamental es que la categorización de delito informático (o de verdaderos "cibercrímenes") solo se relacione con el nuevo bien jurídico de la información y los datos. De esta forma, su posición es conforme con la del legislador colombiano, que configuró nuevos tipos penales —informáticos— bajo esta misma egida.

En relación con las características propias de la criminalidad informática, POSADA MAYA reseña lo que considera son características inherentes de los riesgos que

[33] POSADA MAYA. *Los cibercrímenes, cit.,* pp. 99-100.
[34] POSADA MAYA. *Los cibercrímenes, cit.,* pp. 101-102, 103-104.

este tipo de criminalidad generan, es decir, las características de los riesgos informáticos[35]:

i. Son riesgos automáticos, en cuanto que las conductas punibles son ejecutadas mediante tratamientos automatizados, lo que les permite a los atacantes la posibilidad de realizar agresiones informáticas complejas de manera simultánea y repetida.

ii. Son riesgos descentralizados, ya que el objeto del ataque —la información y los datos— se encuentra descentralizado, en manos de terceros, de tal suerte que el titular de estos puede que no se entere de la lesión que está sufriendo.

iii. Son riesgos anónimos, dada las herramientas que el Internet otorga para poder permanecer bajo una identidad oculta.

iv. Son riesgos técnicos, ya que suceden en un contexto informático, el cual las más de las veces comporta determinadas características técnicas que implican un desfase entre lo regulado por el derecho y lo que realmente sucede en ese contexto.

v. Son riesgos masivos o de efectos catastróficos, en cuanto que un ataque puede generar profundas consecuencias de desestabilización social o económica.

vi. Son riesgos propios de la criminalidad organizada trasnacional, trasfronteriza y corporativa, considerándose que el cibercrimen también busca el provecho económico, directo o indirecto, explotando los mercados ilícitos, dinámicos, digitales y asimétricos; que su ejecución implica un bajo costo operativo a la par de una gran ganancia ilícita; que metodológicamente los ciberdelitos también tienen como base el reconocimiento, la infiltración y la búsqueda de la impunidad; que la dañosidad y alcance de estas conductas es catastrófica, por lo que pertenece a la categoría de la macrocriminalidad; y por último, considerando que hay una criminalidad instrumental de delitos medio a delitos fin.

En conclusión, para POSADA MAYA debe distinguirse radicalmente entre los delitos que usan los sistemas informáticos o a los computadores como medio para la comisión de delitos, de los verdaderos delitos informáticos, que son aquellos en

[35] POSADA MAYA. *Los cibercrímenes, cit.,* pp. 53-65.

los cuales hay riesgo o lesión para la información y los datos. Lo anterior no solo porque la verdadera criminalidad informática conlleva unas características que no son compartidas por otros tipos de criminalidad, sino porque sería una ampliación conceptual excesiva incluir como cibercrimen lo que es un delito tradicional expandido por las nuevas posibilidades tecnológicas.

3. El doctrinante argentino ABOSO presenta una posición cercana a la de SUÁREZ SÁNCHEZ y POSADA MAYA. La posición de ABOSO parte del reconocimiento de la gran transformación que implicó en la sociedad postindustrial el surgimiento de las tecnologías de la información y las telecomunicaciones. A la par de ese vertiginoso desarrollo, se empezaron a presentar desafíos inéditos para el arsenal represivo del derecho penal, que no conocía estas nuevas formas de ataques cibernéticos a los sistemas informáticos que venían simplificando las formas de vida de los asociados.

> "Así surgió en el horizonte normativo del Derecho Penal una nueva forma de criminalidad asociada al uso de las redes telemáticas (*Computerkriminalität*), o bien contra los propios sistemas, programas y datos informáticos, que si bien en algunos casos representaban nuevas modalidades de conductas antijurídicas ya conocidas, por caso, la estafa, en otros supuestos fue necesario ampliar o directamente reformular los extremos de lo injusto típico para abarcar esta novedosa forma de criminalidad informática."[36]

En este sentido, ABOSO sostiene que los sistemas telemáticos representan en el moderno mundo digital un objeto digno de tutela penal. Sin embargo, el reconocimiento de esa forma novísima de criminalidad que lesiona o pone en peligro intereses necesitados de protección penal implica que deba existir una distinción entre el objeto de agresión y el medio utilizado para la comisión de estos "delitos informáticos". Así, señala que cuando el objeto de la agresión informática son la integridad y el funcionamiento de los sistemas automatizados de procesamiento de datos, debemos hablar de "delitos cibernéticos propios o en sentido estricto"; por otro lado, si estamos hablando del uso de la computadora como mero instrumento para llevar adelante acciones disvaliosas contra bienes jurídicos individuales o colectivos, debemos referirnos a esas conductas como "delitos cibernéticos impropios o en sentido amplio"[37]. Lo anterior es una posición cercana a la expuesta por POSADA MAYA en nuestro medio.

ABOSO sostiene que su clasificación es acorde con la descrita por la doctrina anglosajona, en donde se relaciona a los delitos que emplean a las nuevas tecnologías con los delitos de fraude y se les llama *computer assisted crimes*, los

[36] ABOSO, Gustavo Eduardo. *Derecho penal cibernético,* Buenos Aires, B de F, 2018, p. 16.
[37] ABOSO. *Derecho penal cibernético, cit.,* p. 17.

que se diferencian de aquellos en que el objeto propio del delito son los sistemas o redes informáticas, llamados *computer related crimes*[38].

De esta manera, ABOSO no comparte que se extienda mucho el entendimiento de los delitos vinculados mediatamente a las nuevas TIC como "delitos cibernéticos" o "delitos informáticos" —expresiones que utiliza como sinónimos—, sosteniendo que si bien es correcto considerar que los "delitos informáticos" pueden lesionar la propiedad o la intimidad, "una acepción amplia de la criminalidad cibernética impide descubrir una nueva realidad social que impone al Derecho Penal modificar y adecuar su arsenal represivo de cara a los nuevos desarrollos tecnológicos alcanzados por la humanidad"[39], con lo que quiere decir que involucrar las nuevas formas en que los viejos delitos se están ejecutando al círculo restringido de los delitos cibernéticos "propios" puede tener como consecuencia la imposibilidad del derecho penal para identificar cuál situación corresponde con la nueva realidad lesiva y cuál no.

Finalmente, también como lo hacen los autores colombianos reseñados más arriba, trae colación una serie de características que a su juicio identifican a la criminalidad cibernética, las cuales, al mismo tiempo que son los rasgos distintivos de estas formas de ataque, también son los mayores desafíos para gestionar, enfrentar y solucionar por parte de las autoridades estatales. Ellas son[40]:

i. El anonimato, que cubre con un halo de misterio a los agresores y les facilita escapar de la persecución judicial.

ii. El bajo costo, que motiva la comisión de los ilícitos, ya que la ejecución de actos disvaliosos no requiere de grandes inversiones económicas o de esfuerzo para lograrse.

iii. La vulnerabilidad de los sistemas y redes telemáticas, que se hace evidente por la gran dependencia que la sociedad de la información respecto de los sistemas y redes informáticas.

iv. La posibilidad de ejecutar delitos a distancia que generan conflictos jurisdiccionales, lo que no ha sido debidamente gestionado por la cooperación internacional, permitiendo que la impunidad se acreciente en relación con las conductas cibernéticas.

---

[38] *Ídem.*
[39] ABOSO. *Derecho penal cibernético, cit.,* p. 18, n. 35.
[40] ABOSO. *Derecho penal cibernético, cit.,* pp. 28-58.

4. La posición de SAIN —también argentino— es diferente a la de SUÁREZ SÁNCHEZ, POSADA MAYA y ABOSO, en cuanto que, de forma más amplia, considera que delitos informáticos son aquellas "conductas indebidas e ilegales donde interviene un dispositivo informático como *medio* para cometer un delito o como *fin* u *objeto* del mismo."[41] Como ejemplo, señala que el primer caso se da cuando una persona intimida o intenta chantajear a otra persona vía correo electrónico, siendo el dispositivo informático el medio de comisión del delito; a su vez, el segundo caso sucederá cuando el dispositivo informático es el objeto del ataque, como cuando un sujeto envía un virus a la computadora de un tercero para dañarla o alterar su funcionamiento.

Asimismo, al considerarse que existen múltiples definiciones de delito informático en la actualidad, según SAIN hay cuatro características que la mayoría de las conceptualizaciones de delitos informáticos introducen. Así, señala como primera característica que debe ser *legal*, es decir, estar consagrado en la ley penal; en segundo lugar, debe ser *técnico*, es decir, vinculado a un dispositivo electrónico, informático o computacional; en tercer lugar, debe tener un determinado *entorno*, esto es, suceder en un espacio específico, que será el Internet o el ciberespacio; finalmente, en cuarto lugar, el delito informático requiere de *la aplicación de técnicas y herramientas informáticas en el proceso de investigación*[42]. Señala, además, que la mayoría de los delitos informáticos son anónimos, trasnacionales e inmediatos, y que, si bien anteriormente requerían de *hackers* para su comisión, hoy "cualquier persona con conocimientos básicos en computación puede cometer un delito informático"[43].

Concluye este autor argentino señalando que la ambigüedad de la definición del delito informático se ve reflejada en los nombres de las unidades investigativas que se han venido creando para combatir esta criminalidad, ya que se les han denominado unidades de "delitos informáticos", "cibercrimen", "delitos tecnológicos", "crímenes cibernéticos", "delitos telemáticos", "crímenes electrónicos", "delitos de alta tecnología", o "crímenes por computadora".

5. Tal vez la posición más ajustada a los nuevos tiempos de las redes sociales y del desarrollo comunicativo y social en Internet sea la presentada por el español MIRÓ LLINARES, quien se decanta por la adopción de un concepto de "cibercrimen" —el cual utiliza como sinónimo de "cibercriminalidad"— que englobe

[41] SAIN. "Internet, el cibercrimen y la investigación criminal de delitos informáticos", *cit.,* p. 8.

[42] SAIN. *Ob. Cit.*, pp. 9-10, no comparte la cuarta característica, puesto que es una realidad que la implementación de pericias forenses de tipo informático o digital se realizan en la actualidad en una multiplicidad de casos no informáticos, como, por ejemplo, en las investigaciones de homicidios cuando se realizan recuperaciones de información producto de la trasmisión de datos a través de redes de comunicaciones con el fin de establecer indicios sobre la conducta.

[43] SAIN. "Internet, el cibercrimen y la investigación criminal de delitos informáticos", *cit.,* p. 11.

no solo los ya clásicos ataques informáticos (denegación de servicios, intruismo, propagación de *malware*, *et ál*) sino también las nuevas formas lesivas que han surgido en los últimos años a partir de introducción de la Web 2.0 y las subsiguientes generaciones de Internet.

Para MIRÓ LLINARES el concepto de cibercrimen se ajusta más al fenómeno delictivo de hoy, superando la denominación de "delitos informáticos", la cual, reconoce, todavía se usa extendidamente en el derecho español[44], a partir de la insoslayable influencia alemana en ese ordenamiento. Así, los trabajos de SEIBER y de ROMEO CASABONA, en Alemania y España, son los que ayudaron a popularizar esas expresiones relacionadas con la informática.

Sin embargo, el autor comentado señala que tanto "delitos informáticos" como "cibercrimen" o "cibercriminalidad" son expresiones que no hacen referencia a un bien jurídico concreto, sino que se refiere más bien a un *ámbito de riesgo informático o cibernético*, dentro del cual se despliegan las más variadas conductas, las cuales pueden ser nuevas y desconocidas, o viejas ajustadas a nuevas formas comisivas que mutan los límites materiales de sus injustos[45].

En este orden de ideas, considera que las posibles lesiones o puestas en peligro que surgen en el mundo virtual van más allá del objeto de protección de la información y los datos. Así, adoptando la terminología señalada y desplazando a la de "delito informático", se hace posible introducir bajo ese parangón a todas las conductas que hoy están lesionando intereses en el ámbito virtual, sin que sean solo considerados como "verdaderos cibercrímenes" los que se relacionen con la pureza informática.

> "Al fin y al cabo, si bien Internet, la Red más popular y a través de la cual se realizan prácticamente todas estas infracciones, es en sí misma un medio informático y, por tanto, todos los ciberdelitos podrían entrar dentro de la categoría de los delitos informáticos, con la utilización del término cibercriminalidad se pone de manifiesto que sus implicaciones de riesgo van más allá de la utilización de las tecnologías informáticas y se relacionan mucho más con el hecho de que estos comportamientos están unidos en la actualidad a redes telemáticas, con los particulares problemas político-criminales que ello plantea en la actualidad. Además, al tener en cuenta no solo el aspecto 'informacional' sino también el comunicativo de las TIC, se hace referencia a un catálogo más amplio de infracciones que incluye las que se relacionan con el (mal) uso de las comunicaciones personales entre particulares a través de redes telemáticas o con la introducción y mala utilización de contenidos introducidos en ellas."[46]

MIRÓ LLINARES reconoce la validez de los conceptos amplios y restringidos de cibercrimen. Como otros, también entiende al cibercrimen amplio como el que

[44] MIRÓ LLINARES. *El cibercrimen, cit.*, p. 37.
[45] MIRÓ LLINARES. *El cibercrimen, cit.,* p. 36.
[46] MIRÓ LLINARES. *El cibercrimen, cit.,* pp. 38-39.

vincula viejas y nuevas conductas a las TIC y al ciberespacio. A su vez, el concepto restringido de cibercrimen solo les otorga ese mote a las conductas que antes del Internet, las TIC y el ciberespacio no existían. Así, dentro de la concepción amplia, por ejemplo, el *child grooming*[47] podrá ser ciberdelito si se ejecutó a través del medio cibernético. Por el contrario, no lo será en una concepción restringida, la cual aceptará como ciberdelito conductas como la denegación de servicios, pero no otras que antes del desarrollo tecnológico ya existieran con una contraparte física.

Sostiene MIRÓ LLINARES que lo determinante para definir un ciberdelito es que las TIC tengan tal incidencia en el comportamiento desviado que le otorgue un elemento especial.

> "Eso sí, para que estemos ante un cibercrimen no bastará con que se utilicen las TIC para realizar el comportamiento criminal, sino que se exigirá que tal uso tenga que ver con algún elemento esencial del delito."[48]

De esta forma, no es cibercrimen imprimir una carta con amenazas para ejecutar una extorsión, pero sí lo será realizar amenazas de que devendrá un mal para la víctima si no se pliega a las exigencias del autor, cuando lo realiza mediante un correo electrónico, o cuando se logra la disposición fraudulenta mediante un engaño desplegado utilizando el medio virtual. En este sentido, entiende "por cibercrimen cualquier delito en el que las TIC juegan un papel determinante en su concreta comisión, que es lo mismo que afirmar que lo será cualquier delito llevado a cabo en el ciberespacio, con las particularidades criminológicas, victimológicas y de riesgo penal que de ello se derivan."[49]

Por lo anterior, MIRÓ LLINARES reconoce una clasificación de los cibercrímenes en los cuales se introducen no solo las conductas que antes de la Revolución Tecnológica no eran posibles, sino también las viejas (que llama "ataques réplica"), en cuanto que estas viejas conductas ejecutadas por estos nuevos medios conllevan consecuencias criminológicas diferentes a si se hubieren cometido sin la ayuda de las TIC.

De acuerdo con su clasificación[50], que atiende al grado de incidencia de las TIC en la comisión del hecho, podemos entender los cibercrímenes como:

---

[47] La conducta consiste en contactar menores por medio de redes sociales u otras formas de comunicación como salas de chat, mensajería instantánea, o incluso mediante la comunicación verbal física, con el fin de ganar su confianza y ejecutar un posterior abuso sexual (Corte Suprema de Justicia, Sala de Casación Penal. Sentencia SP4573-2019, radicado No. 47234, M.P.: Eugenio Fernández Carlier).

[48] MIRÓ LLINARES. *El cibercrimen, cit.,* pp. 41.

[49] *Ídem.*

[50] MIRÓ LLINARES. *El cibercrimen, cit.,* pp. 51-116.

- Ataques puros, relacionados con las conductas que no existen por fuera del ciberespacio, como el *hacking*, la denegación de servicios o el daño informático.

- Ataques réplica, que hacen referencia a las conductas que existían antes del advenimiento de las TIC, pero que con ellas encuentran nuevas dimensiones criminológicas, como los ciberfraudes económicos, el ciberespionaje, el *phishing*, el *child grooming*, entre otros.

- Ataques de contenido, que también son ataques réplica, pero que sus particulares características imponen un tratamiento diferente, como sucede con las violaciones de derecho de autor, la pornografía infantil o el discurso del odio, en donde surgen problemas criminológicos relacionados con la responsabilidad en cascada, la intervención delictiva, etc.

6. Por otra parte, la doctrina anglosajona ha sido más amplia en su entendimiento del *cybercrime*. Por ejemplo, para THOMAS y LOADER, el cibercrimen puede ser considerado como "actividades mediadas por la computadora que son ilegales o consideradas ilícitas por ciertos sujetos y que pueden ser ejecutadas a través de redes electrónicas globales. Su distinción se deriva de las versátiles capacidades proveídas por las nuevas TIC."[51] En este sentido, THOMAS y LOADER sostienen que es a través de las TIC y del Internet que las organizaciones criminales pueden diseñar técnicas más sofisticadas de delitos tradicionales, como el tráfico de droga, el lavado de activos, el tráfico de armas, el contrabando, entre otros.

Empero, esto no quiere decir que consideren a estos delitos clásicos como cibercrímenes. Contrario a ello, señalan que para entender esta nueva cibercriminalidad no es suficiente pensar en los viejos delitos ejecutándose de nuevas formas.

> "Los cibercriminales, como el mismo cibercrimen, están marcados por una transformación fundamental en la forma en que pensamos en el problema del crimen y la criminalidad. Actos considerados criminales que simplemente involucran a las TIC son de menos preocupación que aquellos que son posibles solamente por virtud de las TIC. Por ejemplo, el uso de un computador para defraudar a alguien no se diferencia en nada del uso de un teléfono o de una conversación cara a cara para defraudar a alguien. Lo que hace de estos crímenes cibercrímenes es que cuando se usan las TIC se adiciona un elemento significativo al crimen, que hubiera sido imposible sin él."[52]

En este sentido, para THOMAS y LOADER sí debe hacerse una distinción entre la mera instrumentalización de los medios informáticos para la comisión de delitos de los verdaderos cibercrímenes como categoría nueva y autónoma, fundamentado

[51] THOMAS, LOADER. "Cybercrime", *cit.,* p. 3. *(Trad. del Aut.).*
[52] THOMAS, LOADER. "Cybercrime", *cit.,* p. 6. *(Trad. del Aut.).*

en el *plus* que las nuevas tecnologías otorgan a las conductas humanas lesivas o peligrosas para los intereses sociales o individuales.

Sobre la cibercriminalidad, THOMAS y LOADER, en línea con las categorizaciones propias que realiza la criminología, señalan que existen tres categorías básicas de cibercriminales[53]:

i. *Hackers* y *phreaks*, los cuales las más de las veces no buscan provecho económico, a pesar de que sus acciones sí pueden generar daños económicos para las personas o las empresas.

ii. Mercaderes de la información y mercenarios, los cuales mediante acciones de sabotaje buscan infiltrar los sistemas y obtener información para ser después vendida o traficada.

iii. Terroristas, extremistas y desviados, los cuales se embarcan en acciones de ciberterrorismo, de promoción del odio, trasmisión de pornografía infantil o pedofilia en línea. Aquí se incluyen los sujetos que participan de la guerra cibernética o que organizan actividades políticas ilegales de manipulación e infiltración de democracias.

7. Para CLOUGH[54], existen tantos términos para referirse al cibercrimen como existen cibercrímenes. En los albores de los estudios sobre esta problemática, se hablaba de *computer crime* (crimen de computadora), *computer related crime* (crimen relacionado con la computadora) o *crime by computer* (crimen por computadora). Posteriormente, ante el desarrollo tecnológico, se habló de *high technology crime* (crimen de alta tecnología). El advenimiento del Internet introdujo términos como *cybercrime* (cibercrimen), *Internet crime* (crimen de Internet) o *net crime* (crimen de red).

El autor sostiene que, si estos términos se toman literalmente, cada uno de ellos va a sufrir de deficiencias al no incluir elementos o características que soportan su conceptualización. En efecto, si hablamos de delitos computacionales, se está haciendo énfasis en los computadores, lo que deja de lado al Internet o la Red, por lo que no se incluiría en este término los delitos relacionados con esos aspectos. De otro lado, si se habla de cibercrimen o de "crímenes virtuales" puede que se deje de lado conductas que no sucedan en el contexto del Internet o del ciberespacio, así utilicen computadores o sistemas informáticos. Por ello, no debe haber una aproximación literal a estos conceptos, "sino más bien como términos

[53] THOMAS, LOADER. "Cybercrime", *cit.,* pp. 6-8.
[54] CLOUGH. *Principles of cybercrime, cit.,* p. 9.

amplios descriptivos que enfatizan el rol de la tecnología en la comisión del crimen."[55]

En este orden de ideas, para CLOUGH hay un amplio consenso en lo que el término "cibercrimen" comprehende, que incluye la triple clasificación realizada por el Departamento de Justicia de los Estados Unidos[56]:

i. Crímenes en los cuales el computador o la Red es el objeto de la actividad criminal, como sucede en las conductas de intruismo, utilización de *malware* o ataques de denegación de servicio.

ii. Ofensas existentes en las cuales el computador es una herramienta para cometer el delito, como sucede en la pornografía infantil, el acoso, el fraude o las violaciones de derechos de autor.

iii. Crímenes en los que el uso del computador es incidental, pero él puede ser utilizado para obtener evidencias del crimen, como sucede en los casos de homicidio en los que se revisan los dispositivos tecnológicos utilizados por el victimario o la víctima para recolectar evidencia.

Con base en lo anterior, CLOUGH denomina a estas conductas tripartitas como delitos computacionales (*computer crimes*), delitos facilitados por los computadores (*computer facilitated crimes*) y delitos soportados por los computadores (*computer-supported crimes*). Con todo, si bien en su trabajo reseña delitos viejos ejecutados a través de los nuevos medios, CLOUGH señala que "los verdaderos cibercrímenes, en el sentido de ofensas que no existirían sin la computación, son aquellas que se dirigen en contra de los computadores y las redes computacionales como tal."[57] Con ello, podría incluirse a CLOUGH dentro de la categoría de SUÁREZ SÁNCHEZ, POSADA MAYA y ABOSO.

Sobre las características de la cibercriminalidad, el autor comentado considera —como ABOSO— que estas mismas características son a su vez los grandes retos que la legislación debe acometer en su lucha contra los cibercrímenes. En este sentido, las siguientes características de la tecnología digital son las que facilitan la comisión de estos delitos y dificultan el trabajo de persecución de las autoridades estatales[58]:

i. En relación con la escala, a diferencia de otras tecnologías de la comunicación, Internet permite a muchos usuarios comunicarse

[55] CLOUGH. *Principles of cybercrime, cit.,* p. 9. *(Trad. del Aut.).*
[56] CLOUGH. *Principles of cybercrime, cit.,* p. 10.
[57] CLOUGH. *Principles of cybercrime, cit.,* pp. 10-11. (*Trad. del Aut.*).
[58] CLOUGH. *Principles of cybercrime, cit.,* pp. 5-8.

fácilmente y de forma barata. Según ciertas estadísticas citadas por el autor, 1.600 millones de personas en el mundo utilizan el Internet, lo que se comporta como un grupo con gran potencial de convertirse en victimarios o víctimas de conductas en el ciberespacio. Lo anterior les permite a los victimarios realizar conductas con efectos masivos que no podrían ser conseguidos en un ambiente *offline*. Adicionalmente, la posibilidad de automatizar procesos, amplia aún más el efecto multiplicador de la ofensa cibernética.

ii. Sobre la accesibilidad, para comprender gráficamente su implicación, basta recordar como hace algunos años los computadores eran grandes máquinas que ocupaban cuartos enteros y a los cuales solo accedían los agentes del Gobierno o las grandes empresas. Hoy, los dispositivos informáticos caben en un bolsillo y es casi seguro encontrar uno en cada persona adulta. De esta forma, se puede afirmar que la tecnología es ubicua y cada vez más fácil de usar —cuando no es fácil de usar, existen tutoriales en Internet que desmenuzan de forma práctica cómo hacerlo— asegurando así su disponibilidad tanto para las víctimas como para los victimarios.

iii. Relativo al anonimato, la criminología de antaño ha identificado esta característica como atractiva para el ofensor, siendo ella uno de los servicios más comunes en el ciberespacio. Abrir cuentas de correo electrónico sin proveer información real, contratar *re-emailers* (servicios de renvío de correos electrónicos sin proveer identificación del remitente), utilización de *software* para ocultar la identidad, etc., son solo algunos de los mecanismos implementados por los criminales para no dejar huellas y no ser identificados.

iv. En cuanto a la portabilidad y transferencia, se afirma que central para el poder de la tecnología digital es la posibilidad de almacenar grandes cantidades de información en espacios pequeños, y de que sea posible transferir esa información de forma rápida y segura sin que sea demeritada su calidad en ese proceso. Esta posibilidad es campo fértil para una criminalidad que con solo subir una foto en el Internet puede generar un efecto viral lesivo sin precedentes.

v. El alcance global de las tecnologías digitales afecta de forma profunda la pretérita característica del derecho penal como uno de naturaleza local o circunscrito a una determinada jurisdicción. Hoy, las redes globales de la información han desplazado a este paradigma, en cuanto

que los victimarios pueden realizar daño sin estar presentes donde está la víctima, solo necesitando una conexión a Internet.

vi. La ausencia de guardianes capacitados se comporta como un reto para las autoridades, ya que uno de los elementos que motivan a los agentes criminales es la previsión de no ser detectados ni procesados. La gran especialidad de los temas informáticos implica que los investigadores sean igualmente capacitados para recolectar forensemente evidencia digital. Así mismo, debe haber una interlocución entre las autoridades del Estado y los demás actores de este ambiente tecnológico, en cuanto que como sucede en el ambiente fuera de línea, no siempre es deseable que exista un policía en cada esquina, siendo entonces importante la autorregulación, la autoprotección, la colaboración de otro tipo de guardianes (padres, comunidades, prestadores de servicios de internet, etc.) para gestionar los riesgos digitales de la nueva era.

8. Para YAR el estudio conceptual del cibercrimen debe empezar de forma irrestricta por el estudio del Internet y del ciberespacio, ya que, sin ellos, simplemente no se podría hablar de cibercriminalidad. En este sentido, no debe verse al Internet solo como un "pedazo de tecnología" que existe aparte de las personas que lo usan. Contrario a ello, y considerando que es en el ciberespacio en donde ocurren los cibercrímenes, el Internet debe ser visto como un conjunto de prácticas sociales. El Internet toma la forma que tiene es a partir del uso que las personas le dan por los propósitos que ellos buscan.

> "Lo que las personas hacen con la Red, y cómo típicamente se ocupan de ella, son elementos cruciales para entender qué tipo de fenómeno el Internet en realidad es. En efecto, son las clases de usos sociales que le damos al Internet las que posibilitan el surgimiento de actividades criminales y desviadas. Para dar un ejemplo, si las personas no utilizaran el Internet para comprar, entonces no habría ninguna oportunidad para crímenes relacionados con tarjetas de crédito que explotan la información financiera de los usuarios."[59]

A partir de ello, YAR reconoce que las legislaciones no definen el cibercrimen, al no ser específicamente una categoría legal, a pesar de ser ampliamente utilizado en la política, los medios de comunicación, el sistema judicial y las discusiones académicas. Por ello, antes de establecer una definición exclusiva, YAR prefiere y recomienda entender al cibercrimen como "un significativo rango de actividades

[59] YAR, Majid. *Cybercrime and society*, 2nd ed., London, SAGE, 2013, p. 6. (*Trad. del Aut.*).

ilícitas cuyo común denominador es el rol central que juegan las redes de tecnologías de la información y las comunicaciones en su comisión."[60]

En este sentido, YAR no acepta las argumentaciones que no le otorgan autonomía al cibercrimen, considerándolo solo una nueva forma de ejecutar viejos crímenes. Contrario a ello, enfoca su entendimiento en la importancia del ciberespacio como nuevo ámbito de comisión de delitos que nunca habíamos conocido. En este orden de ideas, señala que el ciberespacio tiene profundos efectos en las relaciones sociales, permitiendo la transformación de las formas de ofensa y las formas de victimización. Como sustento de ello, solo basta referirse a la deconstrucción de la convergencia del espacio-tiempo en la ejecución de las conductas delictuales. Al no existir ese tipo de restricción en el espacio cibernético, propio del espacio físico, es posible entonces sostener que las formas de la desviación criminal y de la victimización en el ciberespacio son trascendentalmente diferentes a las del espacio físico, en donde esos actos lesivos están vinculados y sometidos a la realidad del espacio-tiempo[61].

9. El Gobierno colombiano también ha definido lo que considera es un cibercrimen, mediante sendos documentos de políticas públicas. En efecto, en el 2011, se definió al ciberdelito o delito cibernético como una "actividad delictiva o abusiva relacionada con los ordenadores u las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito."[62]

Posteriormente, esta definición, de alguna manera simplificada, se vería replicada en otro documento de política pública subsiguiente, al señalarse que el cibercrimen o delito cibernético es el "conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio."[63]

II. Toma de postura: criminalidad cibernética y cibercriminalidad informática

1. Un primer tópico sobre el que se debe tomar postura es sobre el concepto de cibercriminalidad como sinónimo de criminalidad informática. En este respecto, rechazamos este tipo de asimilación, ya que no toda criminalidad que se desarrolle por medio del —o en el— ciberespacio debe considerarse como un

[60] YAR. *Cybercrime and society, cit.,* p. 9. (*Trad. del Aut.*).
[61] YAR. *Cybercrime and society, cit.,* p. 11.
[62] Documento CONPES No. 3701. *Lineamientos de política para ciberseguridad y ciberdefensa*, Bogotá, 14 de julio de 2011, p. 38.
[63] Documento CONPES No. 3854. *Política nacional de seguridad digital*, Bogotá, 11 de abril de 2016, p. 87.

atentado en contra de la información y los datos (que sería la concreta criminalidad informática).

En este sentido, sostenemos que la criminalidad informática es una especie de criminalidad cibernética, ya que ella se vale del ciberespacio para generar resultados lesivos o puestas en peligro antijurídicas en contra de la información y los datos. Con ello, manifestamos que la información y los datos no son medios de comisión de conductas punibles —como sí puede serlo el ciberespacio—, sino que es el objeto de protección de la ley penal (el bien jurídico) en algunos casos de cibercriminalidad, más concretamente, de criminalidad informática. Aquí se vislumbra como claro que la información y los datos como bien jurídico protegido le otorgan una característica especial a este tipo de criminalidad (informática), sin que de ahí sea posible considerar a que toda criminalidad que involucre al ciberespacio sea una criminalidad informática.

Lo anterior no es razón para rechazar la característica de intermedio[64] del bien jurídico información y los datos, en lo relativo a que las conductas que lesionan la información y los datos —es decir, aquellas tipificadas en la Ley 1273 de 2009— las más de las veces tienen efectos pluriofensivos que generan lesión y/o peligro sobre otros bienes jurídicos, de clase individual (por contraposición al bien jurídico de la información y los datos, que es colectivo y recae en cabeza de la sociedad). Esto en cuanto que la existencia de otras criminalidades cibernéticas que no sean informáticas en nada incide sobre la naturaleza de este bien jurídico nuevo y especial, que comporta su propia autonomía frente a los otros bienes jurídicos que la criminalidad cibernética no informática lesiona, los cuales podrán ser bienes jurídicos clásicos-personales o bienes jurídicos también nuevos, individuales o colectivos.

De esta forma, entendemos como válida la crítica del rechazo a identificar toda conducta punible vinculada a la informática (como ciencia de procesamiento de información y datos) con un delito informático, ya que ello sería ampliar mucho ese concepto. Por el contrario, para lograr vasos comunicantes entre conductas autónomas, pero no muy lejanas entre sí, desplazamos el concepto de informática y en su lugar introducimos el de cibernética, el cual es un concepto más amplio que el de informática, y servirá como vaso comunicante entre la criminalidad informática concreta y otros tipos de criminalidad no informática cibernética, sin que ambas dimensiones pierdan su autonomía para ser mezcladas o confundidas. Mientras que la informática es el conjunto de conocimientos científicos que permite el procesamiento de información y datos mediante computadoras, la cibernética se refiere a la realidad virtual en la cual esos procesamientos tienen lugar.

---

[64] SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* p. 126 y ss.

Así, las conductas que buscan excluirse del concepto de delito informático quedan en efecto excluidas por no lesionar ni poner en peligro a la información y los datos, sin dejar de perder su caracterización como cibercrímenes o pertenecientes a la cibercriminalidad, por cuanto que ellas también se valen del ciberespacio para existir y, en algunos casos, a partir de su desenvolvimiento en el ciberespacio se tornan en conductas autónomas, nuevas y necesarias de estrategias de prevención nunca implementadas, en cuanto que hasta el advenimiento de las TIC ellas no existían en la forma en que hoy se presentan.

2. El segundo tópico, entonces, se relacionará con la clasificación de los cibercrímenes y los delitos informáticos. Reconocemos que existe razón en no identificar a los delitos computacionales (aquellos tipos penales clásicos en los que se instrumentaliza a los computadores o tecnologías para la comisión del delito) con los delitos informáticos. Empero, nuestra propuesta de clasificación introduce una tercera categoría: los cibercrímenes propios, en contraposición a los cibercrímenes impropios (o delitos computacionales); categorías ambas que se encuentran al lado y a la par de los delitos informáticos.

Es decir, en vez de seguir la clasificación bipartita de POSADA MAYA, adicionamos una categoría más a la clasificación que permite vislumbrar cómo existen diferentes tipos de conductas en las cuales de una u otra manera hay una conexión con la cibernética o el ciberespacio, que es el lugar común en el cual se encuentran, para a partir de ahí comenzar a manifestar sus propias características que les otorgan autonomía o dependencia en relación con conductas clásicas. Por ello, para efectos gráficos, se realiza la siguiente demostración.

La clasificación de POSADA MAYA es la siguiente:

Esta clasificación considera que todos los delitos vinculados al ciberespacio son delitos informáticos, pues da prevalencia al concepto informático sobre el cibernético. Por ello, considera que delitos que no afectan a la información y los datos pero que sí usan el medio del ciberespacio también son delitos informáticos,

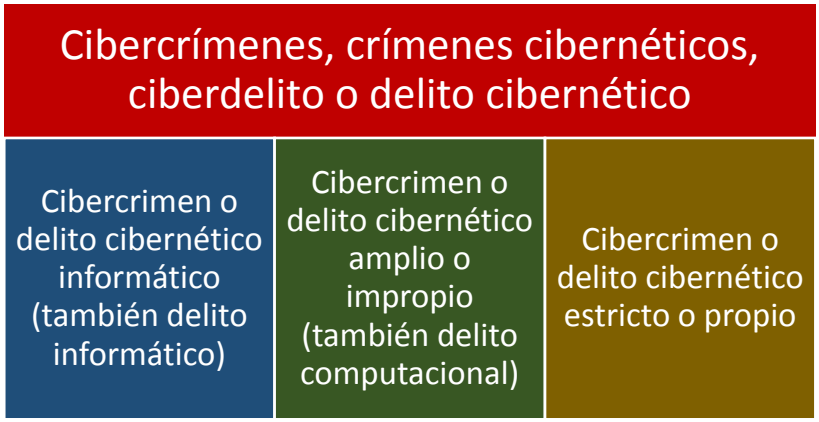
si bien no lo son en sentido estricto, sino amplio. Esta posición es criticable, pues no se encuentra mayor lógica en que un delito que *no es* "informático" —que no lesiona o pone en peligro a la información y los datos— se considere como delito informático.

Otro rasgo importante de esta clasificación es que para darle mayor prevalencia a los delitos informáticos en sentido estricto (o verdaderos delitos informáticos) en contraposición a los delitos informáticos en sentido amplio (o delitos informáticos "aparentes"), se identifica a los delitos informáticos en sentido estricto con los cibercrímenes, que es un concepto descriptivo mucho más fuerte y ajustado a los tiempos modernos que el de simples "delitos computacionales", dejando entonces por fuera de la esfera de los cibercrímenes a delitos computacionales que se valen del ciberespacio para ejecutarse, como la estafa, la extorsión, la injuria, el acoso, etc. —a pesar, se repite, de que sí son delitos vinculados con el ciberespacio—. Esta posición también es criticable, considerando que excluye a delitos relacionados con el ciberespacio por el hecho de no estar vinculados a la información y los datos.

Además, la clasificación de POSADA MAYA comportaría una contradicción en relación con su entendimiento del delito de transferencia no consentida de activos como delito intermedio y el cual considera un "verdadero cibercrimen"[65], es decir, un verdadero delito informático en sentido estricto, pero a reglón seguido señala que es un delito que protege "en primer lugar" —es decir, de forma "directa" o "inmediata"— al patrimonio económico y en "segundo lugar" —esto es, de forma "mediata" o "indirecta"— a la información y los datos, con lo que está otorgando a este delito una característica propia, según su clasificación, de los delitos informáticos "aparentes" o en sentido amplio (esta es, que la protección de los sistemas informáticos es indirecta y la protección de los bienes jurídicos clásicos es directa, y viceversa para los verdaderos delitos informáticos o cibercrímenes)[66].

Por lo anterior, con base en la prevalencia central del ciberespacio sobre la informática como elemento común de estas conductas, nuestra clasificación tripartita es la siguiente:

[65] POSADA MAYA. *Los cibercrímenes, cit.,* pp. 397, 401.
[66] Cfr. *supra*, n. 34.



Esta triple clasificación pone en el centro de gravedad el elemento predominante en las tres categorías: el ciberespacio y la cibernética, y su especial influencia en las relaciones sociales del siglo XXI. Con ello, se logra denominar las tres tipologías como cibercriminalidad o como criminalidad cibernética, en cuanto que las tres se manifiestan en un lugar llamado el ciberespacio. A reglón seguido, cada una de las tipologías recoge una forma de criminalidad cibernética que comporta unos rasgos que la diferencian de la otra.

Empezando con el delito informático o el cibercrimen informático, este tipo de criminalidad se dirige en contra del bien jurídico de la información y los datos[67]. Es decir, es una nueva forma de criminalidad cibernética que tiene una tutela jurídica concreta: la información y los datos. Como ya más arriba se dijo, esto no es óbice para que las conductas que la ley penal tipifica para combatir a esta clase de criminalidad no sean pluriofensivas[68] o sus bienes jurídicos intermedios[69].

---

[67] "El bien jurídico que se protege es el de la relación de confianza que la sociedad debe tener en los sistemas informáticos, las redes de sistemas electrónicos y telemáticos, y otros medios semejantes, es decir, en las tecnologías de la información y las comunicaciones. Se trata, por consiguiente, de un delito que va más allá del interés individual en dicha seguridad, porque la misma le corresponde a la sociedad, la que, además, tiene derecho a la integridad de los datos, la libertad de su procesamiento y comunicación, lo mismo que a la disponibilidad de la información. Por consiguiente, el bien jurídico es colectivo o supraindividual, cuyo titular lo es la sociedad o la colectividad." (SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* pp. 124-125).

[68] De acuerdo con la doctrina (REYES ECHANDÍA, Alfonso. *Derecho penal*, 11ª ed., Bogotá, Temis, 2017, p. 117), una clasificación de los tipos penales es en relación con el bien jurídico tutelado. Desde este punto de vista, los tipos penales pueden ser simples o complejos. Mientras que los simples (o mono-ofensivos) tutelan un solo bien jurídico, los complejos (o pluriofensivos) amparan simultáneamente varios bienes jurídicos. En relación con el carácter pluriofensivo del cibercrimen, cfr. SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* pp. 125-126.

[69] Los bienes jurídicos intermedios (o de índole compleja) son aquellos en los cuales la tutela penal se manifiesta tanto sobre intereses individuales como sobre intereses colectivos, comportándose como herramientas interpretativas adecuadas para determinar el injusto en delitos como los informáticos (cfr. SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* pp. 126-132).

Así, estas conductas, como todas las de la parte especial, dependiendo de su naturaleza y características, pueden o no ser pluriofensivas o protectoras de bienes jurídicos intermedios. En el caso que se estudia, estas conductas son pluriofensivas y protegen bienes jurídicos intermedios porque pueden lesionar o poner en peligro al bien jurídico colectivo al tiempo que pueden lesionar o poner en peligro al bien jurídico individual. Es el caso del acceso abusivo a un sistema informático, el daño informático, interceptación de datos informáticos, la violación de datos personales, la suplantación de sitios web para capturar datos personales, el hurto por medios informáticos o la transferencia no consentida de activos.

En segundo lugar, el cibercrimen amplio o impropio, también llamado delito computacional, hace referencia a todas las conductas clásicas que por su naturaleza modal abierta permiten que la ejecución de la conducta se haga valer de las nuevas tecnologías para lograr su agotamiento, lograr su impunidad, dificultar la persecución judicial, o cualquier otra motivación cuya idea subyacente sea hacer más eficaz y eficiente la actividad criminal, al hacerse valer de ayudas tecnológicas.

Es el caso de las conductas de estafa, extorsión, delitos contra la integridad moral, amenazas, pornografía infantil, violación de derechos de autor, *et ál*. Este tipo de conducta no protege un bien jurídico nuevo, sino a los bienes jurídicos clásicos y la protección que otorga el ordenamiento jurídico no es mediante la creación de nuevas conductas punibles, sino por medio de sanciones agravadas o circunstancias de mayor punibilidad, como sucede en el derecho vernáculo.

De esta forma, de un lado, no se desconoce que esta clase de delitos también involucran en su ejecución al ciberespacio (lo que les permite ser considerados como una especie de cibercrímenes), siendo ello el fundamento que permite su mayor sanción (vía circunstancia de mayor punibilidad), mientras que por el otro se desliga de su identificación —amplia— con el delito informático, pues la lesión o puesta en peligro de la información y los datos en nada se relacionan con este tipo de conducta, excluyendo la posibilidad de que el concepto de delito informático se amplíe hasta abarcar estas conductas, que ciertamente le son ajenas.

Como más adelante se fundamentará, en esta categoría debe introducirse a una especie de acoso, vinculada con el acoso físico-predatorio, que es un verdadero acoso extendido o “derramado” en el ciberespacio (ciberacoso no autónomo o dependiente), que es aquella situación en la cual la conducta de acoso tradicional se extiende y continua en el ciberespacio, como es el caso del ciberacoso doméstico.

Finalmente, nuestra clasificación introduce la categoría del cibercrimen o delito cibernético estricto o propio. Este tipo de delito es una conducta que también se

vincula con el ciberespacio, pues a partir de él el hecho desviado es posible, pero no se relaciona con el bien jurídico de la información y los datos, pues el bien jurídico protegido puede ser uno clásico o uno nuevo, individual o colectivo (por ejemplo, la autonomía cibernética es un bien jurídico individual, mientras que la seguridad pública cibernética —objeto de conductas de ciberterrorismo— es un bien jurídico colectivo, ambos de nueva generación).

Esta categoría obtiene su autonomía del hecho que hay unas conductas que pueden ser muy cercanas a otras conductas clásicas, pero no es posible colocarlas en la clasificación de delito computacional o cibercrimen amplio o impropio porque ellas están dotadas de ciertas características que sus pares clásicos no comportan, al haber evolucionado a partir de un ambiente digital totalmente nuevo.

Así, las nuevas dinámicas que las TIC y el ciberespacio introdujeron en las relaciones sociales, imponen nuevas formas de comportamiento, de lesión, de peligro y de persecución. Estas novedades implican problemas político-criminales propios de estas formas de criminalidad tecnológica (por ejemplo, los problemas sociales y político criminales derivados de las interacciones humanas en la Web 2.0).

Por ello, estas características propias o estrictas de estas conductas les dan una identidad propia que hace necesaria una tipificación aparte, reconfigurando los límites de sus injustos y generando problemas de política criminal que requieren de estrategias focalizadas de prevención y gestión, en cuanto que no es la mera instrumentalización de la tecnología lo que hace necesario un mayor reproche, sino el comportamiento desviado en el ciberespacio, como dimensión comunitaria diferenciable del espacio físico, lo que hace necesaria la intervención del derecho penal.

Si vamos a tomar en serio los efectos de la Revolución Tecnológica en la vida en sociedad, entonces se debe admitir que los cambios generados por la introducción de nuevas tecnologías no se limitan, de un lado, a los atentados contra la información y los datos, y de otro, a la mera instrumentalización medial y modal de la tecnología para cometer delitos. A la par de esa dicotomía, hay que aceptar que se ha creado un nuevo espacio comunitario para la ejecución de conductas valorativas (cerrar negocios, entablar o recuperar amistades, realizar investigaciones) como desvalorativas (el ciberacoso moral, el ciberterrorismo, el *phishing*, el *grooming*, el *sexting*, el *cyber hate speech*, entre otros). En este sentido, hay conductas que han surgido propiamente de las nuevas dinámicas sociales que el ciberespacio ha creado para las relaciones intersubjetivas (cibercriminalidad social o criminalidad cibernética social). Este tipo de relaciones, entonces, requieren de respuestas adecuadas del derecho para promoverlas en

caso de generar valor, o para disuadirlas y sancionarlas, en caso de generar desvalor.

No debe perderse de vista la historia de la informática, el Internet, de las TIC y del cibercrimen para ilustrar la necesidad de conceptualizar estas nuevas conductas evolucionadas. En efecto, en un principio, los sistemas informáticos se comportaban como sitios para acceder y gestionar información. Por ello, la primera generación de delincuencia cibernética fue esencialmente delincuencia informática, en la cual se utilizaban los sistemas informáticos para robar información, destruirla o sabotearla. Seguidamente, con el surgimiento del Internet y de la Web 1.0, se dio paso a una segunda generación de criminalidad cibernética relacionada con la información circulante en la Red de redes, de donde devino la comisión de ilícitos a través de Internet, como la pornografía infantil o la violación de derechos de autor (piénsese, por ejemplo, en los albores del Internet con *Napster*). Aquí se manifestaban los delitos clásicos ejecutados por medio del ciberespacio.

Hoy, y desde hace varios años, estamos inmersos en una Web 2.0 —en realidad, ya contemporáneamente estamos hablando de Web 3.0 o “Internet de las cosas”— la que se ha caracterizado por transformar la forma en que se utiliza el Internet y el ciberespacio, ya no solo para almacenar o acceder a información, sino también para entablar relaciones sociales *personales* no económicas.

Internet y el ciberespacio ya no son lo que fueron al principio a mediados de los noventa o en el cambio de milenio. En aquella época, concomitante con el nacimiento del Internet para el público en general, esa herramienta informática se manifestaba como un excelente medio para acceder a la información y para difundirla, con un valor económico o informacional. Nada de ello es igual hoy en día. La Web 2.0 ha revolucionado el Internet y el ciberespacio para transformarlo en un nuevo ámbito de relaciones interpersonales que antes de las redes sociales y las economías colaborativas era impensable. Por los efectos de la Web 2.0, el ciberespacio hoy no es solamente un lugar para acceder y trasferir información, o para hacer transacciones económicas; más allá de eso, se ha convertido en un ámbito para socializar, relacionarse, contactar viejos amigos, conocer nuevos amigos, buscar pareja, serle infiel a la pareja, jugar juegos, y en general, simplemente *estar* a partir del propio desarrollo vital de lo que significa ser un *ciudadano digital*.

Este ámbito de intercomunicación digital es el que genera valores, protegidos y deseados por los ciudadanos digitales, pero también peligros, que se ciernen sobre ellos y sus bienes personales más preciados; y si ello es así para la mayoría de los seres humanos que se conectan al ciberespacio, será aún mayor para los

denominados “nativos digitales”, sujetos que desde su nacimiento *nunca* han conocido un mundo desconectado.

Algunos, como ABOSO, haciendo valer su preocupación por la extensión desmedida de un entendimiento de “verdadero delito informático” o “verdadero cibercrimen”, señalarán que esta clasificación, en efecto, ha extendido en demasía lo que debe ser entendido como un cibercrimen. En concreto, ABOSO señala que ampliar mucho el entendimiento de lo que es un delito cibernético impedirá encontrar la nueva realidad lesiva necesitada de regulación[70]. Empero, nuestra posición es diametralmente la contraria: no ampliar la conceptualización a los nuevos fenómenos de la criminalidad en la Web 2.0 y de la criminalidad cibernética social implicará el desconocimiento de conductas disvaliosas que generan un gran impacto y daño a los miembros de las cibercomunidades.

En este sentido, ignorar que han surgido —o mejor: evolucionado— conductas clásicas a partir de la especial incidencia de las TIC y del ciberespacio en la forma de su comisión y victimización (el elemento especial que reclaman THOMAS y LOADER para considerar a un delito “ciberdelito”), solo con el afán de mantener la pureza de las conductas que no se conocían antes de esa misma Revolución Tecnológica, se presenta como una posición que dejaría desprotegidas a poblaciones vulnerables frente a amenazas reales y tan cibernéticas como lo pueda ser el acceso abusivo a un sistema informático o la denegación de servicios.

3. Un tercer tópico sobre el que hay que tomar postura en este capítulo es sobre las características propias de la criminalidad cibernética. Si bien la doctrina ha elaborado listados de características de la criminalidad informática y no de la criminalidad cibernética, debemos aceptar que esos rasgos distintivos aplican también —las más de las veces— a la criminalidad cibernética en los términos de nuestra clasificación, por lo que se puede afirmar que esos rasgos que se ven como exclusivos de la criminalidad informática por algunos doctrinantes, en realidad son rasgos de la criminalidad cibernética, y por esa vía, son rasgos propios de los tres tipos de criminalidad cibernética (la amplia, la estricta y la informática). Sin embargo, ello no significa que no existan algunos rasgos que sean propios de la criminalidad informática y sí sean excluyentes a los otros dos tipos de criminalidad cibernética, como que algunas características de éstas sean solo de su resorte, y no alcancen a caracterizar a la criminalidad informática.

Consideramos, siguiendo a varios de los autores citados, que son rasgos distintivos a toda la criminalidad cibernética, los siguientes:

---

[70] Cfr. *Supra,* n. 39.

i. La automatización. Esto quiere decir que todos los riesgos que involucren a la tecnología cibernética son riesgos automatizados, ya que mediante el conocimiento especializado es posible que a partir de una acción el hecho se pueda repetir múltiples veces, sin mayores instrucciones posteriores.

ii. La gran capacidad de hacer daño. Considerando la interconexión e interdependencia de los individuos con los medios tecnológicos, los ataques cibernéticos, en contra de las personas o de la información y los datos, tienen la potencialidad de generar grandes daños, tanto físicos, psicológicos y económicos. Así, existe una asimetría entre ofensores y los resultados, ya que un solo agente puede hacer tambalear a toda una sociedad o a un Estado.

iii. La facilidad para encubrir el delito. Dada la alta complejidad de que implica el uso de tecnologías para cometer delitos, un conocimiento especializado otorga mayores herramientas a los criminales para encubrir sus rastros.

iv. El anonimato. Es una característica propia del ciberespacio y del Internet, que se convierte en un atractivo para los criminales y significa uno de los elementos fundamentales de las diversas teorías etiológicas que buscan explicarlo como configurador de muchos hechos delictivos, al permitir que ciudadanos que no actúan de determinada manera en el mundo físico, lo hagan en el mundo virtual.

v. El distanciamiento entre autor y víctima. Es un rasgo común, e incluso deseable por los criminales, la existencia de una gran distancia entre el lugar en donde el agente empieza la ejecución del hecho y el lugar en donde el resultado o el peligro se manifiestan, que es en el espacio que ocupe la víctima.

vi. La gran potencialidad transfronteriza del delito. No compartimos, como señalan algunos autores, que el delito cibernético sea *per se* transfronterizo[71]. En lugar de ello, reconocemos la gran potencialidad del punible de trascender fronteras, ya que la deslocalización del ciberespacio y la posibilidad del distanciamiento entre autor y víctima, son circunstancias que permiten que el delito se torne transfronterizo.

[71] Así, POSADA MAYA. *Los cibercrímenes, cit.,* p. 65. También SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* p. 47.

Empero, se reitera, ello no es siempre así, con lo que con la fórmula de la potencialidad no se descartan ciberdelitos que suceden, muchas veces, dentro de la misma jurisdicción territorial de un ordenamiento jurídico.

vii. La alta cifra negra. Es una característica propia de la criminalidad cibernética no solo por los rezagos en las capacitaciones de las autoridades (que deben ser constantes), sino también por la desestimación de conductas potencialmente peligrosas o lesivas que se consideran menores por todavía existir prejuicios en cuanto a la capacidad de daño de los medios tecnológicos y de la existencia de bienes jurídicos tradicionales o nuevos que se ven afectados por conductas desplegadas en el ciberespacio.

viii. La accesibilidad. La ubicuidad del Internet y la simplicidad y relativa gratuidad para acceder al ciberespacio otorgan como rasgo distintivo el hecho de que la criminalidad cibernética o mejor, la posibilidad de generar una criminalidad cibernética, es accesible a una gran cantidad de personas, que para llevar a cabo sus conductas solo requieren del dispositivo y su conexión. Desde la perspectiva victimológica, la accesibilidad también se manifiesta, ya que de la misma manera en que fácilmente acceden al ciberespacio los ciberdelincuentes, también lo hacen las cibervíctimas.

Descartamos como características distintivas de la criminalidad cibernética que sea propia de la criminalidad económica, corporativa y/u organizada —como lo propone POSADA MAYA[72]—, ya que, si bien en esos escenarios se puede manifestar este tipo de crímenes, no es cierto que este sea un rasgo que los defina, en cuanto que muchos *hackers*, *crackers* o ciberdelincuentes actúan por su propia cuenta, en solitario, solo con la ayuda de su computador y de una conexión a Internet. Lo anterior no es óbice para aceptar que existen organizaciones criminales o grupos delictivos dedicados a la criminalidad cibernética en alguna o todas sus formas. Empero, se reitera, no porque ello sea así puede sostenerse que *toda* criminalidad cibernética (e informática, incluso) sea también criminalidad económica u organizada.

También descartamos —como lo reseña SAIN[73]— que la criminalidad cibernética para ser tal deba estar tipificada en la ley, porque ello sería una posición

[72] POSADA MAYA. *Los cibercrímenes, cit.,* p. 65.
[73] SAIN. "Internet, el cibercrimen y la investigación criminal de delitos informáticos", *cit.,* p. 9.

reduccionista de un positivismo arcaico, que la criminología rechaza; tampoco aceptamos, como este mismo autor reseña, pero enseguida rechaza, que la criminalidad cibernética requiera de técnicas de investigación forense-digital de forma exclusiva, porque ese rasgo aplica a cualquier tipo de criminalidad.

CAPÍTULO SEGUNDO

Conceptos de (ciber)acoso y (ciber)hostigamiento

I. Acoso y acoso en línea

A. Panorama y prevalencia de la problemática

El ciberacoso y el ciberhostigamiento —tratados por la mayoría de autores como sinónimos— se han manifestado como problemas sociales serios y de consecuencias lesivas graves para las víctimas que los sufren. A pesar de la falta de violencia física en la ejecución de la conducta[74], ella puede tener un serio impacto sobre la salud psicológica de la víctima, mediante la generación de miedo, ansiedad, depresión, desordenes de sueño, pensamientos suicidas y estrés postraumático[75].

Gran debate genera este tópico, en punto sobre lesividad de conductas que incluso pueden considerarse halagadoras o inocuas. Al respecto, surge como necesario resaltar el carácter repetitivo y persistente de la conducta, que es lo que al final dota a la acción de su potencialidad dañina y lesiva.

> "Tal reiteración y persistencia genera la sensación de pérdida de control de la víctima, a lo que se añade la sensación de ineficacia de la respuesta del sistema de justicia penal o de otras instancias de ayuda a la víctima, lo que vulnera la creencia de la víctima de estar viviendo en una sociedad segura y la conduce a la ruptura de sus expectativas de recuperar el control."[76]

Si bien la conducta ciberacosadora se relaciona con muchos casos de violencia de género y abusos domésticos, ella también se puede desarrollar por fuera de esos contextos, en especial la conducta *online* en contraposición con el acoso *offline*, tradicional o físico. En todo caso, se ha identificado que la conducta acosadora y ciberacosadora puede comportarse como un preludio a la ejecución de violencia física por parte del victimario en contra de la víctima o de alguien conocido por la víctima[77], en especial en los casos de abuso doméstico, violencia intrafamiliar y feminicidios[78].

---

[74] Empero, como adelante se detallará, ciertos autores como ROYAKKERS categorizan algunos tipos de violencia física (como el asalto) como formas de *stalking* o acoso.

[75] HOFFMEISTER, Thaddeus. "Legislative reactions", en NAVARRO, Jordana N.; CLEVENGER, Shelly; MARCUM, Catherine D. (eds.). *The intersection between intimate partner abuse, technology and cybercrime*, Durham, Carolina Academic Press, 2016, p. 195; CLOUGH. *Principles of cybercrime*, p. 366.

[76] VILLACAMPA ESTIARTE, Carolina. *Stalking y derecho penal,* Madrid, Iustel, 2009, pp. 107-108.

[77] PITTARO, Michael L. "Cyberstalking: typology, etiology and victims", en JAISHANKAR, K. (ed.). *Cybercriminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011, pp. 278, 283; CLOUGH. *Principles of cybercrime, cit.,* p. 366.

[78] CRISAFI, Denise N.; MULLINS, Alyssa R.; JASINSKI, Jana L. "The rise of the virtual predator: technology and the expanding reach of intimate partner abuse", en NAVARRO, Jordana N.; CLEVENGER, Shelly; MARCUM, Catherine D. (eds.). *The intersection between intimate partner abuse, technology and cybercrime*, Durham, Carolina Academic Press, 2016, p. 115.

En relación con la violencia de género[79], se ha documentado que el ciberacoso y el ciberhostigamiento son conductas que hacen parte del problema estructural de violencia en contra de la mujer, cuya complejidad crece mediante el uso de la tecnología. En América Latina, la situación es grave, en cuanto que existe una ausencia de marcos legales adecuados y de interpretaciones judiciales que den respuesta a las víctimas sin afectar otros derechos humanos, como la libertad de expresión. Se ha concluido, también, que existe una falta de capacitación de los funcionarios públicos que atienden estos casos, los cuales, siguiendo los prejuicios comunes de la violencia de género, los minimizan o archivan sin mayores investigaciones o análisis[80].

Otro grupo que comúnmente sufre las consecuencias criminales y lesivas del ciberacoso y del ciberhostigamiento son los periodistas[81], especialmente los periodistas de investigación y las periodistas en general (siendo objetos comunes de ataques las periodistas deportivas que con su oficio violentan los roles de género). En Francia, gran revuelo mediático[82] causó el caso de "La Liga del LOL", un grupo de periodistas que se dedicaban a ejecutar sistemáticamente conductas de ciberacoso y de ciberhostigamiento en contra de sus colegas mujeres, realizando montajes fotográficos sexuales, esparciendo rumores y atacando su aspecto físico.

Una de las grandes conclusiones del informe publicado por la oenegé Reporteros Sin Fronteras en el año 2018 es que el fenómeno es mundial y se presenta en forma de métodos de represión estatales tanto en países autoritarios (China, Rusia, India, Turquía, Vietnam, Argelia, Irán) como en países clasificados como democráticos (como Francia, Suecia, Finlandia, México, Colombia). La consecuencia más inmediata de este tipo de conductas sobre los periodistas es la autocensura y el cierre de cuentas virtuales, lo que repercute negativamente en la solidez del Estado de derecho.

Un tercer grupo vulnerable frente a las conductas de ciberacoso y ciberhostigamiento son los menores, niños, niñas y adolescentes que no solo sufren estos ataques en el ámbito escolar o a manos de sus pares, en lo que serían casos de acoso escolar, matoneo o *bullying*, sino también en contextos escolares a manos de sus superiores o en contextos no escolares a manos de

---

[79] Cfr. PEÑA OCHOA, Paz (ed.). *Reporte de la situación de América Latina sobre la violencia de género ejercida por medios electrónicos*, Fundación Karisma *et ál*, noviembre de 2017, *pássim*. Accesible en: [https://karisma.org.co/descargar/latin-american-report-on-online-gender-violence/]

[80] *Ídem,* p. 3.

[81] Reporteros Sin Fronteras. *Acoso en línea a periodistas: cuando los trolls arremeten contra la prensa*, 26 de julio de 2018, *pássim*. Accesible en [https://rsf.org/es/noticias/rsf-publica-su-informe-acoso-en-linea-periodistas-cuando-los-trolls-arremeten-contra-la-prensa]

[82] [https://www.france24.com/es/20190213-ligalol-periodistas-acoso-mujeres-internet]

desconocidos. En el contexto escolar, en Colombia es paradigmático el caso del estudiante Sergio Urrego, el cual fue objeto de acoso y hostigamiento de parte de las directivas del colegio en el cual estudiaba por motivo de su orientación sexual, lo que lo llevó a suicidarse[83]. Por fuera del contexto escolar, los fenómenos globales de "La Ballena Azul"[84] y de "Momo"[85] se comportan como ejemplos del alcance lesivo de las conductas acosadoras y hostigadoras de grupos criminales transfronterizos, incluso automatizados, en contra de los menores.

En este orden de ideas, puede afirmarse que las conductas de ciberacoso y ciberhostigamiento son conductas socialmente desviadas, que se facilitan por las tecnologías de la información y las comunicaciones para ocultar trazos de identificación del autor, generar un mayor impacto y llegar a un mayor número de víctimas. Si bien este tipo de conductas tienen una íntima relación con situaciones de violencia de género o violencia en contra de parejas o exparejas sentimentales, también es cierto que ese no es el único contexto en el que las tecnologías son instrumentalizadas para generar daño personal a las víctimas, ya que el Internet y las redes sociales también han permitido que estos criminales ataquen a otros grupos de sujetos con los cuales ni siquiera han conllevado una relación personal real o física, como sucede en los casos de los periodistas y los menores. Sin embargo, la conducta tampoco se limita a ellos, en cuanto que cualquiera puede emprender la conducta de hostigamiento en contra de cualquier víctima seleccionada al azar.

Los países que más atención le han dado a este fenómeno han sido Estados Unidos, Gran Bretaña y Australia. Seguidamente, en Europa continental también se han proferido leyes sobre el asunto. Sobre los estudios empíricos, ha sido en Estados Unidos, y en menor medida en Gran Bretaña, en donde se han recogido y analizado la mayoría de las muestras que pueden llevar a conclusiones sobre la realidad de la prevalencia del problema del acoso. En Estados Unidos, la *National Violence Against Women Survey*, encuesta realizada entre noviembre de 1995 y mayo de 1996 sobre dieciséis mil personas, fue uno de los instrumentos más importantes para sacar conclusiones sobre el acoso en esa nación[86]. Otros

---

[83][https://www.elespectador.com/noticias/bogota/caso-sergio-urrego-otro-fallo-historico-contra-la-discriminacion-articulo-829555]

[84] [https://www.bbc.com/mundo/noticias-46974250]

[85] [https://www.telemundo51.com/noticias/destacados/Reto-Momo-crea-proecupacion-entre-los-padres--506468141.html]

[86] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* pp. 68-69.: "Partiendo de exigir que la víctima padeciera un elevado nivel de temor, la encuesta informó que un 8% de mujeres en USA y un 2% de los hombres habían padecido *stalking* alguna vez en su vida, lo que significa que una de cada 12 mujeres norteamericanas (8,2 millones) y uno de cada 45 hombres (2 millones) han sufrido *stalking* en algún momento de sus vidas. De éstos, el 90% había sido victimizados por un único *stalker*, mientras que un 9% de mujeres víctimas y un 8% de hombres víctimas lo había sido por dos o más ofensores, reduciéndose al 1% el

estudios posteriores también se han realizado en Estados Unidos, Gran Bretaña, Australia y algunos países europeos[87].

En Colombia no existen cifras compiladas sobre este fenómeno criminal, lo que explicaría la ausencia de regulación legislativa, en cuanto que no se cuentan con datos concretos, más allá de los compilados de forma general por las oenegés, en especial en el tema de la violencia de género.

Lo anterior pone de presente las dificultades que las políticas públicas y criminales deben acometer para buscar disuadir la comisión de estos hechos y sancionar en el marco del derecho penal mínimo y garantista a los autores de estos ataques, habida cuenta que lo que se reseña comúnmente como acoso o ciberacoso, hostigamiento o ciberhostigamiento, son conceptos difusos y maleables que se presentan en diversas situaciones, muchas veces lejanas o disímiles entre sí, lo que, a la postre, también afecta la recopilación y consolidación de cifras. De ahí la necesidad de realizar conceptualizaciones criminológicas concretas de las diversas situaciones, con el fin de lograr una política legislativa concreta y acotada que no violente derechos fundamentales como la libertad de expresión ni garantías fundamentales como la tipicidad estricta.

B. Antecedentes históricos-legislativos

La conducta de acoso como forma de acecho o como forma de hostigamiento moral no están tipificadas en la ley penal colombiana (más allá de los antecedentes de las conductas de los artículos 210A y 134B del Código Penal, circunscritas, en el primer caso, a la motivación sexual y, en el segundo, a la instigación de la discriminación). Los antecedentes históricos de la figura (en especial de su forma de acecho predatorio) se remontan a los inicios del siglo XVIII, en Inglaterra, cuando en 1704 un sujeto conocido como el Dr. Lane perseguía constantemente a su víctima, la señorita Denis. El caso ha sido condensado de la siguiente manera:

> "Un doctor, el Dr. Lane, perseguía constantemente a la Señorita Denis. La madre de ésta le prohibió acercarse a ella, orden que fue desatendida por el sujeto. En consecuencia, madre e hija decidieron trasladarse a Londres. Sin embargo, dicho intento de perder el rastro del Doctor fue fallido, pues este se trasladó también a la ciudad londinense y se alojó en el mismo hotel, en la habitación contigua a la de madre e hija.
>
> A la mañana siguiente, cuando la señorita Denis se dirigía a su vehículo con su chofer, el Doctor golpeó a éste con el objetivo de forzar a la víctima a irse con él. Este suceso fue objeto de litigio judicial y a la salida de la celebración de dicho juicio el Doctor hirió gravemente al

---

porcentaje de víctimas que habían sufrido ataques por parte de tres personas distintas." Estas cifras aumentaron sustituyendo el requerimiento de generación de un nivel elevado de temor por un nivel medio.

[87] Cfr. la reseña de las cifras de prevalencia en VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* pp. 78-93.

> abogado defensor de Denis. Ello produjo un nuevo pronunciamiento judicial en el que se condenó al sujeto a lo que en nuestro ordenamiento jurídico equivaldría a una orden de alejamiento de un año y un día."[88]

Otro caso sucedió un poco más de un siglo después, en 1840, también en Inglaterra, conocido como el caso *Regina v. Dunn*. El caso se condensa así:

> "Dunn era un abogado que dedicó a perseguir durante un año a Angela Coutts. Todo comenzó con el envío de cartas y continuó con el envío de una tarjeta de presentación al hotel donde ella se alojaba. Ángela decidió cambiar de hotel al ver dicha tarjeta, lo que propició que Dunn le enviara cartas de forma continuada, además de aproximarse físicamente a ella e intentar acceder al edificio donde aquella vivía. Coutts denunció los hechos y le impusieron a Dunn una orden de arresto en diciembre de 1838. Al salir de prisión, continuó con el envío masivo de cartas, lo cual provocó en Coutts una sensación de miedo e incertidumbre, llegando incluso a temer por su vida. Sin embargo, al denunciarlo, el tribunal consideró que no había pruebas suficientes para entender efectiva la amenaza, ya que no se tenía en cuenta el patrón de conducta del sujeto activo."[89]

Solo hasta 1990 se tipificaría por primera vez en el mundo la conducta de *stalking* o de acoso, cuando el estado de California la sancionó[90] a partir del caso de la actriz Rebecca Sheaffer, quien fue asesinada en 1989 por Robert John Bardo, un fan que llevaba tres años siguiéndola, enviándole cartas y acudiendo a un sitio de rodaje con regalos y un cuchillo.

A partir de allí, paulatinamente todos los cincuenta estados y el Distrito de Columbia en Estados Unidos tipificaron la conducta de acoso[91]. En el mundo, también se encuentra sancionada en Inglaterra, Canadá, Australia, Alemania, Austria, España, Portugal e Italia[92].

Con el advenimiento de las TIC, se hizo necesario legislar sobre el ciberacoso o el acoso cibernético o ejecutado mediante dispositivos electrónicos. En este sentido, dos posiciones se presentaron al respecto —las cuales tienen estrecha relación con el importante debate sobre la autonomía o no de la conducta de ciberacoso respecto del acoso tradicional—: de un lado, los que ajustaron la conducta tradicional de acoso para introducir el acoso mediante sistemas electrónicos, y de

---

[88] ÁLVAREZ ÁLVAREZ, Suleima. *Consideraciones sobre el nuevo delito de acoso*, San Cristóbal de la Laguna, Universidad de la Laguna, 2016-2017, p. 5.

[89] LORA MÁRQUEZ, Marian. *Estudio jurídico doctrinal del delito de acoso o stalking*, Sevilla, Universidad Internacional de la Rioja, 2017, p. 8.

[90] LORENZO BARCENILLA, Silvia. *Stalking. El nuevo delito de acecho del art. 172 ter del Código Penal*, Barcelona, Universidad Oberta de Catalunya, 2015, p. 33; CLOUGH. *Principles of cybercrime, cit.,* p. 365; ÁLVAREZ ÁLVAREZ. *Consideraciones sobre el nuevo delito de acoso, cit.,* pp. 6-7; LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso o stalking, cit.,* p. 9.

[91] PITTARO. "Cyberstalking", *cit.,* p. 292.

[92] CLOUGH. *Principles of cybercrime, cit.,* pp. 368-371; LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso o stalking, cit.,* pp. 47-51.

otro, los que legislaron conductas autónomas de ciberacoso, a la par del acoso tradicional, pero no dentro de él.

Como ejemplo del primer caso están los estados de California y Montana, que introdujeron dentro de la descripción típica clásica del acoso a los "medios electrónicos". Como ejemplo de lo segundo está el estado de Illinois, que proveyó una conducta autónoma de ciberacoso en su legislación[93].

En el derecho continental europeo, en específico en el ordenamiento español, se discute si el tipo penal de *stalking* cubre el acecho realizado por medio electrónicos. Según la doctrina y la jurisprudencia, la respuesta parece ser afirmativa, en cuanto que es un tipo penal de medios abiertos y todas las conductas que ese artículo enlista —a excepción de la cercanía física— pueden ser ejecutados mediante medios electrónicos[94].

C. Acoso y hostigamiento (*online* y *offline*). Conceptos y delimitaciones

El objeto del presente acápite es reseñar las conceptualizaciones sobre el acoso, el hostigamiento, el ciberacoso y el ciberhostigamiento, y el debate sobre la autonomía o no de las conductas cibernéticas en relación con sus pares fuera de línea. Como se verá, muchos autores equiparan el acoso con el hostigamiento, o consideran que uno es el género y el otro la especie (o viceversa). Otros los consideran diferentes, si bien al momento de enfrentar sus conceptualizaciones es difícil determinar en qué consiste la diferencia. Más aún, otros consignan la palabra "hostigamiento" dentro de las definiciones de acoso, como una forma de acotar ese término. Sin embargo, son muchos más los problemas que estas palabras encuentran en la tarea de su conceptualización.

En relación con la conceptualización del acoso, la problemática ha sido harta compleja, en cuanto que, en un primer lugar, existe el choque entre el concepto social y el concepto legal, lo que viene a complicarse más con la introducción de conceptos clínicos (psiquiátricos o psicológicos) de la conducta. Como bien se sabe, los conceptos legales responden a las necesidades propias de cada legislación y de cada situación contextual de los ordenamientos jurídicos. Así, algunos ordenamientos exigen resultados naturales para la comisión de la conducta, mientras que otros solo exigen resultados jurídicos de peligro. También, algunas legislaciones señalan una lista taxativa de actos que pueden ser acoso o ciberacoso, mientras que otras solo presentan cláusulas generales. Otras exigen un número determinado de actos para configurar un patrón de conducta o incluso

[93] LORENZO BARCENILLA. *Stalking, cit.,* p. 38.
[94] LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso o stalking, cit.,* pp. 43-44.

exigen que se realicen amenazas “creíbles” para que el acoso o el ciberacoso puedan ser sancionados. En todo caso, la conceptualización científico social no necesariamente debe responder a esos parámetros legislativos.

Es importante resaltar que la conceptualización prejurídica es esencial para poder acotar los límites entre lo que después —en sede legal— será prohibido y sancionado. De ahí la importancia de realizar un esfuerzo conceptualizador que permita diferenciar las acciones socialmente adecuadas (en especial cuando inocuas o no concatenadas) de las que comportan una relevancia penal desde la perspectiva de la teoría del bien jurídico (esto es, cuando lo lesiona o lo pone en peligro).

Empero, los ya difíciles retos de lograr la conceptualización se verán agravados por las situaciones de pánico moral y por el rol que la *mass media* ejerce en los temas que llaman la atención y el morbo de la ciudadanía en general. No debe perderse de vista como la construcción social del problema del acoso ha sido permeado —e incluso impulsado— por el cubrimiento de los medios masivos de comunicación de los casos de celebridades. De ahí que en un primer momento de la identificación y construcción del problema a finales de los años ochenta y principios de los noventa en California, pasará por la identificación de estos casos casi que exclusivamente con las celebridades. Solo subsiguientes etapas de acotamiento, estudios e investigación estadística llegarían a relacionar el problema del acoso también con personas del común y en especial con la violencia de género y doméstica.

VILLACAMPA ESTIARTE[95] explica con claridad esta temática. Parte de la idea de que los problemas sociales, desde una perspectiva constructivista, no surgen de la nada, sino que siempre están latentes, solo que llegan a un punto de ebullición en el cual la sociedad les presta la atención adecuada, sea por medio de su reconocimiento legal o simplemente porque entra en el debate público. En relación con el acoso, VILLACAMPA ESTIARTE resalta como hay noticia de estos sucesos desde hace harto tiempo y para su comprobación, recuerda los casos ya reseñados sucedidos en la Inglaterra del siglo XVIII y XIX. Más allá, ahonda en ciertos arquetipos bíblicos y literarios para denotar que el asunto no es nuevo. Así las cosas, identifica tres etapas de la construcción social del problema del acoso.

En una primera etapa, en los años ochenta, que denomina pre-*stalking*, la batuta la llevaban los medios de comunicación, que reporteaban más que todo los casos sufridos por mujeres. En esta etapa se perfiló al acosador como hombres compulsivos, obsesivos, con bajo registro sexual, escasa autoestima, responsables de su comportamiento y con fines sexuales o amorosos en la

[95] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* pp. 57-63.

ejecución del acoso. La segunda etapa vendría con el asesinato de la actriz Rebecca Schaeffer, con lo que se inicia la etapa de "emergencia del *stalking*". En este contexto, el delito se vinculó con las celebridades y se caracterizó al acosador como un desequilibrado mental. Finalmente, la tercera etapa de construcción social del acoso se dio a partir de 1992-1994, cuando los estudios feministas empezaron a vincular la conducta dominadora del acoso con la violencia basada en prejuicios de género. Aquí, el acosador se perfiló como un hombre machista, expareja, que busca mantener su dominio sobre la mujer.

Con base en lo anterior, podemos afirmar que la conceptualización del acoso y la perfilación del acosador no han sido fáciles. Contrario a ello, considerando que hay diversos tipos de violencia que se vinculan a la conducta (violencia de género, violencia aleatoria, violencia producto de trastornos), se torna complicado delimitar y acotar desde la política legislativa qué es lo que se quiere disuadir, proteger o sancionar. Con ello, la necesidad de esfuerzo por lograr un concepto de acoso y de ciberacoso (junto con uno de hostigamiento y ciberhostigamiento que sirva también de referencia conceptual) se torna más imperativa, ya que, a partir de los estudios cuantitativos de prevalencia, es imposible sostener la no lesividad de la conducta, a la vez que, a partir de nuestro irrestricto compromiso con el derecho penal mínimo y democrático, no es dable expandir inadecuadamente el derecho penal mediante la sanción de actos que no reportan afectación de un bien jurídico determinado.

Como se indicó, el primer interés en la construcción social del concepto de acoso fue dado por los medios masivos de comunicación a partir de casos concretos que revertieron el interés de la sociedad por este tipo de conducta. Seguidamente, el segundo interés en estas acciones desviadas devino de la psicología y de la psiquiatría, al identificarse al sujeto acosador con el desequilibrado mental.

1. Así, una de las conceptualizaciones más divulgadas del acoso desde esta perspectiva médica, fue la delineada por MELOY y GOTHARD en 1995. De acuerdo con estas autoras, la conducta acosadora —denominado por ellas como *obsessional following*— consiste en "un patrón de amenaza o acoso anormal o de larga duración dirigida específicamente a un individuo."[96]

[96] MELOY, J. Reid; GOTHARD, Shayna. "Demographic and clinical comparison of obsessional followers and offenders with mental disorders", en *American Journal of Psyquiatry*, No. 152:2, American Psychiatric Association, February 1995, p. 259. *(Trad. del Aut.).* [Accesible en http://drreidmeloy.com/wp-content/uploads/2015/12/1995_DemographicandC.pdf].

Consideran MELOY y GOTHARD que el patrón de amenaza debe consistir en más de un acto —por lo menos dos— manifiesto de persecución no querida por la víctima que es percibida por ésta como hostigador[97].

En este orden de ideas, el interés de MELOY y GOTHARD es desde la perspectiva clínica. Sin embargo, como será constante en las definiciones, se hace énfasis, de un lado, en la repetición de la conducta, y de otro, en el rechazo de la víctima de dicha persecución.

En su trabajo clínico no hay mención del ciberacoso por parte de estas autoras, tal vez, dada la época de su estudio, donde la penetración de las nuevas tecnologías aún no había sucedido.

2. También en el ámbito clínico de la psiquiatría, PATHÉ y MULLEN construyeron un concepto de acoso según el cual este acto consiste en "una constelación de comportamientos en los que un individuo inflige a otro repetidas y no deseadas intrusiones o comunicaciones."[98] Con ello, se vislumbra que el aspecto central de su definición viene dado por las *intrusiones* que el agente proyecta en la víctima.

Dichas "intrusiones" fueron caracterizadas por los autores como persecuciones, merodeos, vigilancias y acercamientos, además de comunicaciones a través de cartas, teléfono, correo electrónico, grafitis o notas adjuntas a, por ejemplo, la entrada de la vivienda o el carro de la víctima[99].

Surge aquí como llamativo que, si bien los autores señalan que no son conductas que hagan parte del núcleo del concepto de acoso, no deben perderse de vista las actividades asociadas al mismo, como pueden ser ordenar bienes a nombre de la víctima, daño a su propiedad, realizar acusaciones, proferir amenazas o incluso atacar físicamente[100].

En relación con el número de conductas necesarias para considerar cumplido el requisito de "patrón de conducta", si bien en un principio en su primer estudio no hicieron mención alguna sobre ello, posteriormente señalaron que la conducta de *stalking* consistía en los intentos repetitivos (por lo menos en diez ocasiones) y

---

[97] MELOY, GOTHARD. "Demographic and clinical comparison of obsessional followers and offenders with mental disorders", *cit.,* p. 259.

[98] PATHÉ, Michele; MULLEN, Paul. "The impact of stalkers on their victims", en *British Journal of Psychiatric*, No. 174, Royal College of Psychiatrist, 1997, p. 12. *(Trad. del Aut.).* [Accesible en https://www.cambridge.org/core/journals/the-british-journal-of-psychiatry/article/impact-of-stalkers-on-their-victims/77725274AFEF6AC57AD59113F47C3BBD]

[99] MULLEN, Paul; PATHÉ, Michele; PURCELL, Rosemary. *Stalkers and their victims*, Cambridge, Cambridge University Press, 2000, p. 7.

[100] PATHÉ, MULLEN. "The impact of stalkers on their victims", *cit.,* p. 12.

persistentes (por lo menos durante cuatro semanas) de aproximarse o comunicarse con la víctima en contra de su voluntad[101].

Como los autores anteriores y tal vez por las mismas razones, PATHÉ y MULLEN no reseñan en su trabajo conceptualización alguna del ciberacoso.

3. WESTRUP y FREMOUW, también desde la literatura clínica, trajeron a colación su definición de *stalking*. Parten de demandar una mayor precisión del concepto, ya que el término es indiscriminadamente usado tanto para señalar el acto de perseguir obsesivamente como para en compasar una serie larga de comportamientos que no son precisamente persecutorios (idea crítica que adoptamos y desarrollamos en nuestra toma de postura).

En concreto, señalan que el *stalking* es un comportamiento o una constelación de comportamientos que: (i) se dirigen repetitivamente en contra de un individuo concreto (el objetivo); (ii) son experimentados por éste como intrusivos y no deseados; y (iii) se considera que pueden causar miedo o preocupación en la víctima[102].

Los autores no comentan conductas de acoso ejecutadas mediante elementos tecnológicos.

4. ROYAKKERS, ya desde la perspectiva jurídica, ha propuesto una definición del acoso que lo vincula con las motivaciones subjetivas del autor, en concreto, con motivaciones afectivas y/o sexuales. Así, este autor señala que el acoso es "una forma de agresión mental, en la que el autor irrumpe de manera repetida, no deseada y perjudicial en la vida de una víctima con la que no tiene —o ya no tiene— relación alguna, con una motivación que tiene que ver directa o indirectamente con la esfera afectiva."[103]

Sobre la repetición de la conducta, señala que el acoso debe ser llevado a cabo por el ofensor en un período de al menos seis meses y con una frecuencia de por lo menos dos veces por semana[104]. Así mismo, señala que "los actos de hostigamiento" pueden dividirse en ocho categorías: amenaza (comunicaciones

---

[101] MULLEN, Paul; PATHÉ, Michele; PURCELL, Rosemary; STUART, Geoffrey W. "Study of stalkers", en *American Journal of Psychiatric*, No. 156:8, American Psychiatric Association, August 1999, p. 1245. [Accesible en https://ajp.psychiatryonline.org/doi/pdf/10.1176/ajp.156.8.1244]

[102] WESTRUP, Darrah; FREMOUW, William J. "Stalking behavior: A literature review and suggested functional analytic assessment technology", en *Aggression and violent behavior*, No. 3:3, Elsevier, 1998, p. 255. [Accesible en: https://www.researchgate.net/publication/257525614_Stalking_behavior_A_literature_review_and_suggested_functional_analytic_assessment_technology]

[103] ROYAKKERS, Lambers. "The Dutch approach to stalking laws", en *Berkeley Journal of Criminal Law,* Vol. 3, No. 1, Berkeley University of California, 2000, p. 7. *(Trad. del Aut.).* [Accesible en: https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1073&context=bjcl]

[104] ROYAKKERS. "The Dutch approach to stalking laws", *cit.,* p. 4.

amenazantes a la víctima o sus allegados), violencia (asaltos a la víctima, daño en bien ajeno), terrorismo telefónico (llamadas silenciosas durante la noche), pedidos/correo (comunicaciones amorosas o pedido de bienes a nombre de la víctima), persecución (acecho, aparecer donde está la víctima o esperarla a donde va a llegar), difamación (falsas acusaciones), violación de domicilio y hurto[105].

En cuanto al ciberacoso, reconoce el impacto de la *Word Wide Web* en la vida de las personas, señalando que ella ha contribuido al aumento de una "nueva variante" del acoso, denominada *cyberstalking*, consistente en persecución electrónica, el acoso por correo electrónico y el tormento vía Internet. En estas situaciones, no existen barreras geográficas o físicas, con lo que se facilita la intrusión en la vida de la víctima. Además, "En el Internet, los individuos pueden hablar y escribir sin detección, permitiendo a los acosadores escapar de su responsabilidad por publicaciones negligentes o abusivas."[106]

5. Según CLOUGH, el uso de la palabra acoso es reciente en el contexto legal, siendo la primera referencia de dicho término en el *Oxford English Dictionary* en 1984. En su opinión, el acoso (*stalking*) así como el *shoplifting* (hurto de pequeña cuantía en tiendas), el *hooliganism* (hooliganismo o barras bravas del fútbol) y el *vandalism* (vandalismo) son más que categorías legales, conceptos descriptivos[107]. En términos generales, define el acoso como "un curso de conducta en el cual un individuo inflige en otro intrusiones y comunicaciones repetitivas no deseadas, hasta tal extensión que la víctima teme por su seguridad."[108]

Considera que el acoso es un fenómeno complejo que incluyen un gran espectro de motivaciones, como los celos, el resentimiento, la obsesión o el deseo de ejercer control. El acosador puede ser un conocido de la víctima, una expareja o un completo extraño. CLOUGH reconoce que, aunque en sus inicios la conducta se relacionaba popularmente con los famosos y celebridades, hoy está acreditado que su ocurrencia más común es en el marco de la violencia y el abuso doméstico[109].

La conducta puede tomar una variedad de formas, como el seguimiento, la vigilancia, el hostigamiento repetitivo de llamadas, correos electrónicos o cartas, el dejar material ofensivo para la víctima en su domicilio o buzón, e incluso el daño

---

[105] *Ídem.*
[106] ROYAKKERS. "The Dutch approach to stalking laws", *cit.,* pp. 1-2. *(Trad. del Aut.)*
[107] CLOUGH. *Principles of cybercrime, cit.,* p. 365.
[108] *Ídem*. *(Trad. del Aut.).*
[109] *Ídem.*

en bien ajeno, siendo lo esencial del hecho no tanto las acciones concretas como la repetición de dichas acciones[110].

Sobre los elementos constitutivos de la conducta, señala que son tres. En primer lugar, el elemento conductual[111], que hace referencia a ejecutar un "curso de conducta" o "patrón de conducta", esto es, que se realicen varios actos repetitivos e insistentes. Si bien ello varía de legislación en legislación, lo común es que un curso o patrón de conducta requieran de, por lo menos, dos actos como mínimo. Sobre cuáles actos constituyen acoso o ciberacoso en concreto, señala que, de un lado, rechaza las listas taxativas de conducta, en cuanto que son muy rígidas y pueden dejar por fuera del enfoque de la ley penal conductas que van surgiendo a la par de las nuevas tecnologías; y de otro, también rechaza una descripción excesivamente abierta que no señale en alguna medida cuáles son conductas constitutivas de acoso, por cuanto que ello violaría el principio de precisión de la ley (o en nuestro medio, el principio de tipicidad estricta). Por ello, opta por una solución intermedia, según la cual es adecuado realizar listas de comportamientos delictuales, introduciendo una cláusula general abierta del tipo "actuar de cualquier otra manera en que se pueda razonablemente causar aprehensión o miedo en la víctima por su seguridad o por la de otra persona", lográndose el objetivo de la precisión y la flexibilidad necesaria para que la ley no se quede rezagada frente a los retos constantes que el desarrollo tecnológico le impone al derecho.

En segundo lugar, el elemento del conocimiento de la prohibición (*fault element)*[112]. Sobre este tópico, CLOUGH resalta que es un elemento de vital importancia para concretar una conducta que podría considerarse como muy amplia, que además sirve para diferenciar al acosador criminal del acosador que no sabe que su conducta lesiona los intereses del sujeto que persigue, al ser su intención, a veces bajo determinación de algún desorden psiquiátrico, la de establecer una relación de amistad o amorosa. Así, las dos modalidades de introducción de este elemento pueden ser la subjetiva o la objetiva. Será subjetiva si se introduce en la provisión una calificación de la clase "actuar con dolo" o "actuar con culpa" al momento de ejecutar el curso de conducta. Será objetiva si se introduce una fórmula del tipo "sabía o debía saber" que su conducta generaría un resultado lesivo.

En tercer lugar, el resultado, consistente en el impacto sobre la víctima[113]. En su entender, CLOUGH sostiene que este elemento también concreta la conducta criminal. El resultado de la acción supone que la víctima sea colocada en estado

[110] CLOUGH. *Principles of cybercrime, cit.,* p. 366.
[111] CLOUGH. *Principles of cybercrime, cit.,* pp. 371-372.
[112] CLOUGH. *Principles of cybercrime, cit.,* p. 373.
[113] CLOUGH. *Principles of cybercrime, cit.,* p. 374.

de temor por su seguridad o por la de otro. Empero, reconoce la validez de la crítica que señala que el impacto sobre la víctima no debe ser subjetivo, es decir, no debe atender a si la víctima en realidad sufrió el miedo o no, ya que puede haber víctimas que con un umbral de resistencia mayor que no sientan el temor y, por tanto, no se configure el delito. Por ello, acepta que algunas jurisdicciones opten por un test objetivo de modelo diferenciado, en el cual se analiza si razonablemente un hombre medio hubiere sufrido temor por el curso de conducta del agente para considerar como satisfecho el requisito del resultado.

En relación con la autonomía del ciberacoso frente al acoso, CLOUGH sostiene que

> "con riesgo de combinar imprecisión con imprecisión, el ciberacoso es simplemente un término descriptivo para el uso de nuevas tecnologías para los propósitos del acoso; esto es, el uso del Internet, correo electrónico, y otros dispositivos electrónicos de comunicación para acosar a una persona."[114]

En su opinión, si bien el uso de la tecnología en el contexto del acoso no es nuevo —ya que las llamadas telefónicas silenciosas ya han sido establecidas como una forma típica de acoso—, lo cierto es que las nuevas tecnologías han facilitado y expandido la conducta acosadora, por cuanto que el Internet brinda herramientas que facilitan el anonimato de los atacantes y esa misma naturaleza de fácil escondimiento anima al comportamiento desviado, desinhibiendo a los sujetos a comportarse en el ciberespacio de tal manera que no se comportarían en la vida real. Así mismo, el fácil acceso a los datos personales de las víctimas que voluntariamente los cuelgan en Internet y redes sociales facilita aún más el trabajo del ciberacosador, el cual muchas veces no debe recurrir a tácticas informáticas sofisticadas de hackeo para obtener la información necesaria para hostigar a una persona[115].

En este sentido, parece ser que CLOUGH no otorga autonomía al ciberacoso en relación con el acoso y lo considera más bien, a pesar de reconocerle ciertas características propias, una forma de acoso a través de nuevas tecnologías.

6. PITTARO reconoce que después de décadas de estudios es muy poco el consenso sobre el acosador, así mucho menos sobre el ciberacosador[116]. Reconoce, de entrada, que el ciberacoso es una extensión del acoso, pero que ello no implica que sean iguales, pues de la misma manera que conllevan semejanzas, también implican diferencias. En esta forma, existe una gran incomprensión sobre estas conductas ciertamente desviadas, lo que implica un

---

[114] CLOUGH. *Principles of cybercrime, cit.,* p. 366. (*Trad. del Aut.*).
[115] CLOUGH. *Principles of cybercrime, cit.,* p. 367.
[116] PITTARO. "Cyberstalking", *cit.,* p. 278.

desconocimiento y mala interpretación de las tácticas desplegadas por el agente[117].

Por ello, señala que "el ciberacosador es uno que usa el Internet como una arma o herramienta, de alguna clase, para cazar, hostigar, amenazar y generar miedo y trepidación en su víctima a través de tácticas sofisticadas de acoso, que son, en la mayor parte, no entendidas y, en algunos casos, legales." Y más adelante agrega: "El término *ciberacoso* generalmente se refiere al uso del Internet, correo electrónico, u otro dispositivo electrónico de comunicación para crear un nivel criminal de intimidación, hostigamiento o miedo en una o más víctimas."[118]

Según el autor comentado[119], los comportamientos del ciberacosador pueden variar desde correos electrónicos no amenazantes hasta potenciales encuentros mortales entre el acosador y la víctima. En su opinión, de forma incorrecta parte de la doctrina considera que el ciberacoso involucra una obsesión sexual del agente en relación con la víctima, sin que existan estudios conclusivos sobre ello. En cambio, adopta una posición en la que se indica que el ciberacoso, como el acoso tradicional, está motivado más por la hostilidad interpersonal que surge de problemas de poder y control de un sujeto sobre otro sujeto o grupos de sujetos.

Sobre las características comunes entre el acoso tradicional y el cibernético, considera que tanto el comportamiento acosador como el ciberacosador tienen la intención de hostigar, amenazar o intimidar a la víctima; que se motivan por la hostilidad interpersonal hacía la víctima, lo que surge de problemas de control y poder, en vez del lucro económico o sexual; "El ciberacoso, similar al acoso tradicional *offline*, es generado por la rabia, poder, control e ira que pudo haber sido precipitada por las acciones de la víctima o, en algunos casos, por sus inacciones."[120] Para el autor, esta es la característica que más acerca a las conductas, ya que en ambas el ofensor está motivado por un inestable deseo de ejercer poder, control e influencia sobre la víctima[121].

Otras similitudes que se han identificado a partir de estudios realizados en Estados Unidos indican que tanto los acosadores como los ciberacosadores responden con violencia (física o verbal) cuando se les confronta; que, desde la perspectiva personal, este tipo de criminalidad está más cerca de la tipología del crimen de cuello blanco que del ofensor pandillero que opera en el espacio

---

[117] PITTARO. "Cyberstalking", *cit.,* p. 279: "En alguna medida, el ciberacoso es fundamentalmente una extensión del acoso tradicional, en el cual el ofensor utiliza un modus operandi altamente tecnológico para cometer el crimen." *(Trad. del Aut.).*

[118] PITTARO. "Cyberstalking", *cit.,* p. 278. *(Trad. del Aut.).*

[119] *Ídem.*

[120] PITTARO. "Cyberstalking", *cit.,* p. 278. *(Trad. del Aut.).*

[121] PITTARO. *Ob. cit.,* p. 280.

público; que los sujetos que emprenden estas conductas son educados y de clase media alta. No obstante, los estudios son limitados por existir una alta cifra negra, en muchos casos alimentada porque las autoridades consideran al acoso y al ciberacoso como inofensivos a menos que exista una amenaza creíble de por medio[122].

Sin embargo, PITTARO también ha encontrado diferencias entre el acoso fuera de línea y el ejecutado en el ciberespacio. La más obvia hace relación al elemento modal, por cuanto que el ciberacosador se apoya predominantemente en las nuevas tecnologías para ejecutar su conducta hostigadora o intimidatoria. Además, el acoso tradicional es mucho más fácil de perseguir, ya que los acosadores *offline* las más de las veces dejan un sinnúmero de rastros con los cuales pueden identificarse, individualizarse y perseguirse judicialmente. Contrario a ello, el ciberacosador utiliza al ciberespacio como un *safe heaven* (paraíso seguro) que le provee no solo anonimato, sino una pléyade de herramientas idóneas para borrar sus huellas digitales de la escena del crimen virtual[123].

Otra diferencia fundamental, relacionada con las ventajas frente a la persecución judicial entre ambas conductas, es la deslocalización del ciberespacio, que permite al agente estar geográficamente distante[124] de donde se produce la lesión o el resultado criminal de peligro para el bien jurídico —según la posición que se adopte—. Esta diferencia es fundamental, ya que introduce un elemento novedosísimo que impone otra dinámica al desarrollo criminal de la conducta y puede otorgarle en alguna medida cierta autonomía al ciberacoso en relación con el acoso, por lo menos en su dimensión de persecución judicial.

Dos diferencias también fundamentales son, de un lado, que el acosador las más de las veces ha tenido una relación real o imaginada con la víctima, mientras que los ciberacosadores escogen sus víctimas más bien al azar[125]; y de otro, que el acosador actúa las más de las veces individualmente, mientras que el ciberacosador hace llamados a otros usuarios virtuales —ya sea en redes sociales o creando páginas web independientes— para que se le unan en la actividad hostigadora e intimidante, en lo que la cibercriminología anglosajona ha denominado como *stalking by proxy*[126].

7. CRISAFI, MULLINS y JASINSKI indagan sobre las diferencias o similitudes fundamentales entre el acoso y el ciberacoso, reconociendo que el debate doctrinal al respecto no es pacífico. Si bien se ha intentado diferenciar su

[122] PITTARO. "Cyberstalking", *cit.,* p. 279.
[123] PITTARO. "Cyberstalking", *cit.,* pp. 279, 280, 283.
[124] PITTARO. "Cyberstalking", *cit.,* p. 283.
[125] PITTARO. "Cyberstalking", *cit.,* p. 280.
[126] PITTARO. "Cyberstalking", *cit.,* p. 283.

prevalencia, forma de persecución e impacto, consideran que lo cierto es que esas definiciones conceptuales realizadas por los especialistas son las más de las veces discordantes con las prescripciones legales y los criterios utilizados para perseguir criminalmente estos casos[127].

Estas autoras reseñan que, si bien las diversas leyes en los estados de Estados Unidos comportan diferentes definiciones, se puede afirmar que los elementos básicos constitutivos de la conducta acosadora son tres: (i) un patrón de comportamiento obsesivo o no querido por la víctima, (ii) el curso de conducta del agente causa a la víctima temer razonablemente por su seguridad o por la de otros; (iii) el curso de conducta causa estrés emocional a la víctima[128].

Sin embargo, con base en un estudio de 2003, señalan que existen diferencias apreciables entre la conducta de acoso y la de ciberacoso. Por ejemplo, la victimización producida por el ciberacoso es más corta que la del acoso tradicional o las víctimas de ciberacoso no conocen a sus victimarios las más de las veces. Sin embargo, en el marco de la violencia doméstica —que es el enfoque del trabajo de las autoras en comento— no dejan pasar que los abusadores domésticos también utilizan la tecnología para acosar a sus parejas o exparejas durante la relación o cuando la relación ha terminado[129].

Por ello, concluyen que "quizá el ciberacoso no es un nuevo crimen, sino que la tecnología ha creado espacios donde algunos atacan bajo el disfraz del anonimato mientras que otros descaradamente usan tecnologías para abiertamente continuar sus asaltos en sus víctimas"[130]. Así, consideran que el ciberacoso es sinónimo de usar tecnologías para acechar u hostigar a otros[131].

8. NAVARRO considera al ciberacoso como una especie de ciberabuso. Su entendimiento del ciberabuso se fundamenta en el concepto de control coercitivo que ejercen los victimarios sobre sus víctimas con el fin de establecer su dominio y perpetuar sus privilegios de género. Entiende que existen diversas tácticas de coerción, como la violencia física, la violencia psicológica, la intimidación o la exclusión. La táctica de intimidación se logra típicamente a través de la utilización de amenazas, vigilancia o degradación[132], es decir, mediante acoso o ciberacoso.

---

[127] CRISAFI, MULLINS, JASINSKI. "The rise of the virtual predator", *cit.,* p. 113.
[128] *Ídem.*
[129] CRISAFI, MULLINS, JASINSKI. "The rise of the virtual predator", *cit.,* p. 113.
[130] Crisafi, Mullins, Jasinski. "The rise of the virtual predator", *cit.,* p. 114. *(Trad. del Aut.)*.
[131] *Ídem,* p. 101.
[132] NAVARRO, Jordana N. "Cyberabuse and cyberstalking", en NAVARRO, Jordana N.; CLEVENGER, Shelly; MARCUM, Catherine D. (eds.). *The intersection between intimate partner abuse, technology and cybercrime*, Durham, Carolina Academic Press, 2016, p. 126.

NAVARRO reconoce la discusión actual sobre la autonomía del ciberacoso respecto del acoso tradicional; señala dos similitudes fundamentales entre las dos conductas (que significaría que son más cercanas que lejanas), como son (i) que muchos ciberacosadores, como los acosadores, son exparejas de sus víctimas; y (ii) ambas conductas consisten en comportamientos repetitivos que invaden el sentido de privacidad de la víctima y resultan en sentimientos de miedo y amenaza[133]. Por ello, podría concluirse que "el Internet es probablemente solo otro medio por el cual el acoso sucede."[134]

En relación con el ciberhostigamiento, sigue una definición que indica que dicho concepto se refiere a actos tales como mensajes hostigadores, amenazas, manipulación fotográfica, revelación de información personal y suplantación conducida *online* en contra de un individuo o un grupo[135].

De otro lado, considera al ciberacoso como la utilización de las TIC para hostigar o acosar a una persona[136]. En este sentido, parece usar los términos de forma similar e intercambiable, siendo lo relevante que el ciberacoso o el ciberhostigamiento son formas de ciberabuso.

9. HOFFMEISTER[137] apunta que el ciberacoso o acoso *online* se define como el uso de las comunicaciones electrónicas para hostigar a otro. Cuando la conducta se realiza en el contexto de una relación de pareja, puede considerarse como violencia doméstica. Para este autor, la diferencia fundamental entre la conducta punible de amenazas y la de (ciber)acoso es que la última requiere de un patrón de conducta (es decir, que sea repetitiva), mientras que la primera solo requiere de una amenaza para ser perseguida penalmente.

10. MISHRA y MISHRA consideran que el ciberacoso es un nuevo crimen del género del "ciberterrorismo". Definen al ciberacoso como aquella situación en la cual una persona es perseguida y acechada *online*[138]. El objeto del ciberacoso es matonear, amenazar, hostigar o intimidar a la víctima. Así, "es una especie de ciberataque que puede llevar al ciberterrorismo"[139].

MISHRA y MISHRA se adhieren a la siguiente definición de ciberacoso, sostenida por BOCIJ y McFARLANE:

---

[133] NAVARRO. "Cyberabuse and cyberstalking", *cit.,* p. 134.
[134] *Ídem*. *(Trad. del Aut.).*
[135] NAVARRO. "Cyberabuse and cyberstalking", *cit.,* p. 129.
[136] *Ídem,* p. 134.
[137] HOFFMEISTER. "Legislative reactions", *cit.,* p. 194.
[138] MISHRA, Alok; MISHRA, Deepti. "Cyberstalking: A challenge for web security", en JANCZEWSKI, Lech J.; COLARIK, Andrew M. *Cyberwarfare and cyberterrorism*, London, IGI Global, 2008, p. 216.
[139] *Ídem.* (*Trad. del Aut.*).

> "Un grupo de comportamientos en los que un individuo, grupo de individuos u organización, utiliza las tecnologías de la información y la comunicación (TIC) para hostigar a uno o más individuos. Este tipo de comportamientos puede incluir, pero no están limitados a, la trasmisión de amenazas y falsas acusaciones, robo de identidad, robo de datos personales, daño los datos o a los equipos, monitoreo computacional, solicitudes sexuales a menores con propósitos de intimidación y confrontación. Hostigamiento es definido como un curso de acción que una persona razonable, en posesión de la misma información, podría pensar que le causa a otra persona razonable sufrimiento emocional y estrés."[140]

Con ello, aceptan que el ciberacoso puede ser ejecutado por organizaciones en contra de un número plural de víctimas, lo que en el ámbito corporativo puede llevar a una "ciberguerra" entre competidores. También señalan una definición de "hostigamiento", sin evidenciarse cuál es la diferencia crucial con el "acoso".

Estos autores consideran que la víctima del ciberacoso es típicamente nueva en las redes, no conoce los protocolos de seguridad en la interacción con otros en Internet, normalmente son mujeres, niños o personas emocionalmente inestables[141].

Las tres formas primarias de ciberacoso son el acoso mediante correo electrónico, el acoso mediante el Internet o el acoso mediante el control de la computadora de la víctima[142].

A su vez, el ciberacosador puede ser clasificado en tres grupos[143]: el ciberacosador común obsesivo (la expareja que se niega a aceptar el fin de la relación), el ciberacosador delirante (el enfermo mental que piensa que tiene una relación personal con la víctima) y el ciberacosador vengativo (el sujeto que siente rencor en contra de la víctima por sus acciones o inacciones, como un exempleado o una expareja).

También comparten la clasificación del ciberacoso como directo o indirecto[144]. El ciberacoso es directo cuando los mensajes amenazantes, de hostigamiento o intimidación son directamente comunicados a la víctima. Será indirecto cuando se usa el Internet, las páginas web, redes sociales o foros para hostigar a la víctima públicamente frente a terceros.

Sobre la relación de autonomía con el acoso tradicional, opinan que el "ciberacoso puede variar en alcance y severidad y muchas veces se refleja en el

---

[140] MISHRA, MISHRA. "Cyberstalking: A challenge for web security", *cit.,* p. 217. (*Trad. del Aut.*).
[141] MISHRA, MISHRA. "Cyberstalking: A challenge for web security", *cit.,* p. 217.
[142] *Ídem.*
[143] MISHRA, MISHRA. "Cyberstalking: A challenge for web security", *cit.,* p. 218.
[144] *Ídem.*

comportamiento acosador *offline*. Puede ser visto como una extensión del acoso *offline*, sin embargo, el ciberacoso no está limitado por fronteras geográficas."[145]

11. KILEL señala, por otra parte, que el ciberacoso es una forma de *cyberbullying* y que el hostigamiento es una manera de ejecutar el ciberacoso, entre otras.

> "Ciberacoso es una forma de cibermatoneo donde los adultos están involucrados, en contra de un individuo u organización a través del monitoreo, robo de identidad, falsas acusaciones, intimidación y hostigamiento. Esto puede realizarse en línea o fuera de línea."[146]

Posteriormente, señala que el ciberacoso es un "comportamiento repetitivo en contra de un blanco a través de amenazas, uso de información para hostigar, monitoreo, acusaciones falsas, intimidación y robo de identidad", mientras que el hostigamiento es sinónimo de "acoso, importunar o perseguir."[147]

12. HALDER y JAISHANKAR señalan que los cibercrímenes no deben ser circunscritos solo a las conductas de pornografía infantil, *hacking*, o los fraudes cibereconómicos. Existen otros cibercrímenes que atacan a las personas, entre los cuales está el ciberacoso, el cual no ha tenido una definición legal universal, lo que ha sido una de las causas de la alta cibervictimización de las mujeres[148].

Para estos autores, al no haberse definido legalmente el ciberacoso, los ordenamientos —como el de Estados Unidos— lo han tratado como una versión extendida del acoso tradicional, solo que con el uso de tecnologías de la comunicación. De hecho, el término ha sido usado indistintamente como sinónimo de ciberhostigamiento, al punto que "ciberhostigamiento ha sido usado como un término holístico para otras ciberofensas tales como el ciberacoso o incluso la ciberdifamación", aun cuando cada uno de estos términos difiere del otro[149].

Finalizan, entonces, presentando sus definiciones de ciberacoso y ciberhostigamiento como tipologías de victimización de las mujeres en las redes sociales, así:

- Ciberacoso: "La mujer miembro es acosada en todos los grupos a los cuales se integra y los muros[150] de sus amigos son constantemente

---

[145] MISHRA, MISHRA. *Ob. cit.,* p. 218. (*Trad. del Aut.*).

[146] KILEL, Beatrice. *Cyberstalking: Electronic harassing,* Frederick, Zapphire Publishing, 2014, p. 1. (*Trad. del Aut.).*

[147] KILEL. *Cyberstalking, cit.,* pp. 23, 24. (*Trad. del Aut.*).

[148] HALDER, Debarati; JAISHANKAR, K. "Online social networking and women victims", en JAISHANKAR, K. (ed.). *Cybercriminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011, p. 303.

[149] HALDER, JAISHANKAR. "Online social networking and women victims", *cit.,* p. 305. *(Trad. del Aut.).*

[150] El término "muro" o *wall* hace referencia al espacio o área de una página de la red social Facebook en la cual los usuarios "amigos" pueden publicar comentarios en el perfil de ese usuario.

revisados con la esperanza de ver las publicaciones de la víctima en ellas, sus propias publicaciones o sus actividades en línea."[151]

- Ciberhostigamiento: "Esto puede incluir mensajes constantes en la pared del perfil del usuario o a su correo electrónico personal, que son mostrados en el perfil; ser un visitante regular del perfil y dejar mensajes en su pared; envío constante de solicitudes de amistad; integrarse a grupos en los cuales ella sea una miembro; constantemente publicar mensajes estando en desacuerdo con ella; entre otros."[152]

13. Para KREMLING y SHARP PARKER[153] —al igual que la recién comentada KIEL— el género conductual es el cibermatoneo (*cyberbullying*), existiendo múltiples comportamientos o métodos que se encuadran en esa categoría, como el ciberhostigamiento, el ciberacoso, la denigración *online*, la suplantación y la exclusión *online*. Así, definen el *cyberbullying* como el comportamiento intencional y agresivo dirigido a otra persona a través de medios electrónicos.

En relación con el ciberhostigamiento, señalan que involucra el envío de mensajes ofensivos, el intercambio de insultos en un ambiente público, como las redes sociales o un grupo de chat. También se incluye en esta categoría la emisión de mensajes amenazantes. De acuerdo con los estudios citados por las autoras, las mujeres tienden más a realizar actos de ciberhostigamiento en contra de sus pares femeninas, tal vez porque prefieren evitar el conflicto directo y físico[154].

En cuanto al ciberacoso, reconocen la dificultad de estructurar una definición exacta y general, sin embargo, delinean como elementos típicos de la conducta los comportamientos repetitivos y no deseados que son percibidos por la víctima como intrusivos, amenazantes, aterradores u hostigadores[155]. Según los estudios que citan, la conducta es común entre exparejas, los hombres son más proclives a ejecutarla y las mujeres más proclives a ser victimizadas.

Sostienen que el acoso y el ciberacoso comportan similitudes, pero también diferencias, siendo en muchos casos conductas superpuestas, en especial cuando inicia físicamente y se traslada al ciberespacio para reforzar el acto acechador físico.

---

[151] HALDER, JAISHANKAR. "Online social networking and women victims", *cit.,* p. 305. *(Trad. del Aut.).*
[152] HALDER, JAISHANKAR. "Online social networking and women victims", *cit.,* p. 306. *(Trad. del Aut.).*
[153] KREMLING, SHARP PARKER. *Cyberspace, cybersecurity and cybercrime*, *cit.,* p. 82.
[154] KREMLING, SHARP PARKER. *Ob. Cit.,* pp. 82-83.
[155] *Ídem*, p. 83.

14. YAR[156] realiza un estudio amplio de las conductas cibercriminales, señalando que acciones como el ciberacoso o el *grooming*, a diferencia de otras conductas cibernéticas dirigidas contra las personas, tienen la particularidad de dirigirse a una persona en específico, contrario a otras situaciones, como las de ciberodio, en el que la conducta se dirige a un grupo de personas indeterminadas. Así, considera que este tipo de delitos dirigidos a una persona específica pueden desarrollarse como crímenes puros virtuales, o también pueden ser mixtos, cuando sirven como acompañamiento o preparación para una mayor victimización física.

Por lo que se refiere al ciberacoso, señala que puede ser entendido como una variante similar a conductas que tiene lugar en contextos y ambientes no virtuales. Con esto, sitúa al ciberacoso dentro de la conceptualización más general del acoso, entendiéndolo como un "hostigamiento persistente en el cual una persona repetidamente impone a otra comunicaciones o contactos no deseados."[157]

YAR reseña que existen diversas variantes de acoso/ciberacoso[158]. De un lado, indica que existe el "acoso de extraños" (*stranger stalking*), el cual puede ser ejecutado por personas con desórdenes mentales (erotomaníacos) o por personas sanas, siendo el primero más prevalente en el acoso físico y el segundo en el acoso cibernético. Así mismo, a partir del trabajo del feminismo académico y del activismo de los derechos de las mujeres, se han realizado estudios que permiten afirmar la existencia de un "acoso doméstico" (*domestic stalking*), el cual se desarrolla en los contextos de violencia entre parejas o exparejas. Aquí, el ciberacoso se ve como una extensión de una violencia doméstica más general que también incluye al acoso físico. A su vez, también reconoce la existencia de un "acoso de conocidos" (*acquaintance stalking*), en el cual el acoso es ejecutado por personas que conocen a la víctima pero que la víctima no conoce o reconoce, al no tener contacto previo formal con ellos, como, por ejemplo, un colega de trabajo o un vecino del edificio.

YAR apuntala sendos argumentos importantes para entender el fenómeno del acoso y del ciberacoso. De un lado, señala que esta conducta ha sufrido un radical cambio en la percepción cultural, ya que comportamientos que antes eran relacionados con el amor o la galantería, hoy son repudiados y sancionados jurídicamente.

> "De esta forma, lo que hoy es discutido como acoso fue alguna vez presentado en la literatura como una forma idealizada de amor romántico. Así, puede ser que este tipo de comportamiento no haya sufrido un aumento dramático, sino que las formas en las cuales

[156] YAR. *Cybercrime and society, cit.,* p. 128.
[157] *Ídem. (Trad. del Aut.).*
[158] YAR. *Cybercrime and society, cit.,* p. 130.

> culturalmente pensamos acerca de las relaciones interpersonales han cambiado, creando un problema social respecto comportamientos que antes eran tolerados o incluso admirados."[159]

Ahora, si bien YAR vincula al ciberacoso dentro de un entendimiento más general del acoso, ello no quiere decir que no reconozca ciertas particularidades al acoso en el ciberespacio en relación con su contraparte "terrenal", como lo llama. En efecto, reconoce el debate entre la autonomía o no del ciberacoso como nueva forma de desviación criminal, concluyendo que "quizás, desde una perspectiva balanceada, el ciberacoso debe ser entendido como una nueva variante de un patrón de una conducta criminal existente, una que exhibe tanto continuidades como discontinuidades de su contraparte terrenal."[160]

Así pues, YAR señala dos diferencias fundamentales entre el acoso físico y el acoso cibernético[161]. Primero, que el ciberacoso es más propenso a permanecer mediato y a distancia de la víctima. De acuerdo con los datos y casos registrados, el ciberacoso es más probable que comience y termine *online* sin "derramarse" (utiliza la expresión *spilling over*) a contextos terrenales. Así, el ciberacoso las más de las veces comporta como resultado el daño psicológico y no un daño físico.

En segundo lugar, también señala que parece existir una prevalencia en relación con el ciberacoso según la cual esos incidentes se generan más entre extraños, fuera de contextos domésticos o íntimos.

YAR concluye señalando las dificultades de determinar qué conductas son acoso o ciberacoso, considerando profesiones u oficios que de alguna manera circundan esas conductas, como los citadores judiciales, los activistas que protestan en determinados lugares o los periodistas. Estas dificultades, según el autor, surgen precisamente del hecho de que la conducta de acoso incluye un gran rango de acciones o de diferentes comportamientos, de tal suerte que toda prescripción legal debe hacerse en términos amplios, lo que genera un riesgo de afectación de la libertad de acción y de expresión.

15. En el derecho continental europeo, VILLACAMPA ESTIARTE valora la importancia de la fijación de los contornos determinantes de un concepto como el de acoso o *stalking*, con el fin de lograr despejar la nebulosidad y escasa aprehensión que él comporta y así excluir los riesgos de abstracción que no permitan su persecución por las autoridades, en especial las penales, que operan bajo principios rectores de concreción.

---

[159] YAR. *Cybercrime and society, cit.,* p. 131. *(Trad. del Aut.).*
[160] *Ibídem. (Trad. del Aut.).*
[161] YAR. *Cybercrime and society, cit.,* pp. 134-135.

Reconociendo las grandes dificultades que devienen de las múltiples conceptualizaciones que existen de la conducta de *stalking*, VILLACAMPA identifica como elementos prevalentes la persecución repetitiva, obsesiva e intrusiva respecto de una persona[162].

No obstante, acota también que las múltiples definiciones —sociales, legales y clínicas— aportan a la confusión, en cuanto que existe un malempleo de determinados términos que llevan a razonamientos circulares que no cumplen con el objeto de concretar una conceptualización necesaria para agrupar casos y excluir situaciones socialmente adecuadas. En concreto, se refiere al vocablo "obsesivo". Partiendo de la literatura psiquiátrica especializada (el *Diagnostic and Statistical Manual of Mental Health Disorders* de 1994), las obsesiones se han considerado como pensamientos no queridos o intrusivos, sin embargo, en las conceptualizaciones que se han intentado del *stalking* siempre se hace referencia a lo "obsesivo" como algo que es considerado como benigno desde el punto de vista del acosador, siendo vista la obsesión por el objeto no como algo perjudicial. "De ahí que en algunas definiciones la obsesión es justamente la que causa el *stalking* y al sujeto se lo tilda de *stalker* justamente porque solo un obsesivo puede realizar ese comportamiento, incurriendo en un razonamiento circular."[163]

Así, a pesar del debido reconocimiento de las dificultades que conlleva la definición de este término, VILLACAMPA ESTIARTE aventura a señalar que

> "El *stalking* constituye una forma de acoso predatorio. Supone importunar reiteradamente a una víctima que, siendo objeto de una atención no deseada, rechaza las tentativas de relación de un sujeto, el acosador, que puede perseguir con su proceder múltiples objetivos, pero que a menudo consigue perturbar gravemente el desarrollo vital de su presa."[164]

De esta definición es posible extraer elementos determinantes que diferencian la posición de la autora de otras conceptualizaciones que también reseña en su trabajo. La primera, es la exclusión de la persecución con fines sexuales o eróticos, aspecto que se introdujo en muchas definiciones, en especial en los albores del reconocimiento de la problemática en los años ochenta en Estados Unidos, lo que de alguna manera suponía una confusión o una aproximación excesiva entre el acoso genérico y el acoso sexual, primera modalidad reconocida por la mayoría de los ordenamientos jurídicos.

En segundo lugar, es importante resaltar como para VILLACAMPA ESTIARTE la conducta de *stalking* implica una perturbación en el desarrollo vital de la vida de la víctima. Lo anterior cobra importancia en sede de conceptualización —porque otra

---

[162] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 33.
[163] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 34.
[164] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 23.

cosa será el debate dogmático acerca de la necesidad de resultado natural o de resultado jurídico— ya que con ello intenta acomodar a la conducta dentro de la sombrilla del género del acoso psicológico, diverso del acoso moral.

Por acoso psicológico, VILLACAMPA ESTIARTE entiende una forma de violencia psicológica, cuya incidencia directa es sobre el equilibrio emocional de la víctima y en donde se producen sentimientos de desasosiego, preocupación o inseguridad que podrían llevar incluso a un estado clínico de depresión o estrés. Por otro lado, lo que caracteriza al acoso moral es la producción de sentimientos de humillación, degradación o envilecimiento[165]. Para la autora, el *stalking* es más una forma de acoso psicológico que de acoso moral, estando más dentro de la segunda categoría el acoso laboral o el escolar[166].

En relación con el *cyberstalking* señala que "se refiere al acoso producido empleando las TIC, fundamentalmente internet"[167], con lo que se evidencia que su acepción de esa categoría es dependiente del *stalking*.

16. También en el contexto continental europeo, ALONSO DE ESCAMILLA define al *stalking* como "una conducta intencionada y maliciosa de persecución obsesiva (*obsessional following*), acecho o acoso respecto de una persona a la que se convierte en objetivo."[168]

A partir de esta definición concluye que el *stalking* es un patrón de conducta, es decir, una estrategia de hostigamiento anormal, de larga duración y que está dirigida a un sujeto específico. A juicio de la autora, el *stalking* puede adoptar diversas formas, como acercarse, vigilar, perseguir, merodear, aproximarse, comunicar, telefonear, enviar cartas, encargar objetos, allanar la vivienda, efectuar falsas acusaciones, formular amenazas, asaltar a la víctima o retenerla. Con ello, entiende que la conducta puede incluir una serie variopinta de actos que pueden ser de diversa gravedad, algunas delictivas, otras irrelevantes e incluso aceptadas socialmente[169].

En este orden de ideas, ALONSO DE ESCAMILLA considera que los elementos del *stalking* son los siguientes[170]:

i. Que se lleven a cabo una serie de actos concatenados que constituyan un patrón de conducta.

---

[165] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 45.
[166] *Ídem*, p. 46.
[167] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 55.
[168] ALONSO DE ESCAMILLA, Avelina. "El delito de stalking como nueva forma de acoso. El 'cyberstalking' y nuevas realidades", en RIQUERT, Marcelo A. (coord.). *Ciberdelitos*, 2ª ed., Buenos Aires, Hammurabi, 2019, p. 217.
[169] ALONSO DE ESCAMILLA. "El delito de stalking como nueva forma de acoso", *cit.,* p. 217.
[170] *Ídem,* p. 218.

ii. Que sean actos de carácter no deseado por la víctima.

iii. Que los actos produzcan sentimientos de temor, claro malestar, desasosiego, vergüenza, inquietud y/o peligro, entre otros.

Desde la perspectiva criminológica, considera que no es posible realizar una perfilación exacta del acosador, ya que no suele responder a unas características clínicas comunes, siendo difícil poder establecer un cuadro psicológico sobre su personalidad. Así, existen acosadores que creen que la víctima quiere estar con él, o en otras ocasiones, se obsesiona a tal punto que él quiere convencer a la víctima de que esté con él. En otros casos, el acosador persigue a una víctima con la que ha sostenido una relación, negándose a entender que la relación ha terminado[171].

Por *cyberstalking* entiende "una conducta de acoso u hostigamiento repetitivito que se lleva a cabo en contra de la voluntad de la víctima, utilizando alguna de las herramientas que proporciona Internet, como son *e-mail*, *chat*, mensajes de texto, *Whatsapp*, redes sociales como *Facebook* o *Twitter*, *web pages*, o cualquier otro medio de *cyberstalking*."[172]

Así, ALONSO DE ESCAMILLA resalta que esta forma nueva de *stalking* conlleva unas características especiales[173] otorgadas por su propia naturaleza cibernética, siendo relevantes (i) el anonimato, (ii) la situación de poder del victimario propiciada precisamente por el anonimato, (iii) la posibilidad de que la propia víctima proporcione información relevante para el acoso a través de sus redes o identidad cibernética, (iv) la posibilidad de automatizar el ataque, como en los *mail bombings*, (v) la posibilidad de afectar a la víctima mediante manipulación de fotografías que la degraden. Resulta, entonces, determinante como un elemento propio del acoso cibernético la posibilidad de que entre victimario y víctima no haya contacto alguno.

> "El acosador y su víctima podrán verse o no, pero habrá de plantearse que ya no habrá de ser necesario exigir proximidad física entre el acosador y la víctima para satisfacer la definición de acoso. El contacto se produce actualmente de otra manera que resulta igual de intimidante para la víctima, ya que cada vez que tenga que utilizar su teléfono o su ordenador para leer su correo electrónico o para utilizar sus redes sociales, lo hará con temor a encontrar un nuevo mensaje, es decir, sufrirá un nuevo contacto no deseado con el acosador."[174]

---

[171] ALONSO DE ESCAMILLA. ""El delito de stalking como nueva forma de acoso", *cit.,* pp. 218-219.
[172] ALONSO DE ESCAMILLA. *Ob. Cit.,* p. 229.
[173] ALONSO DE ESCAMILLA. *Ob. Cit.,* p. 230.
[174] *Ídem,* pp. 230-231.

17. Más cerca geográficamente de nuestro país, en el derecho argentino, ABOSO reconoce que una de las grandes dificultades en relación con el estudio científico y dogmático del acoso es la dificultad de lograr una definición unánime que abarque todas las tipologías conductuales que esa acción disvaliosa comprehende. Eso sí, previo a realizar un ensayo de definición, deja en claro que, siguiendo su clasificación ya reseñada de los delitos cibernéticos o informáticos, la conducta de acoso *no es* un verdadero delito cibernético, ya que aquellas conductas que se vinculen medialmente con las TIC para realizar el hecho no son delitos cibernéticos auténticos, sino "en sentido amplio".

Con todo, reconoce que el acoso ha sufrido un vertiginoso desarrollo en las formas en como este tipo de violencia se manifiesta, en especial a partir del advenimiento de las nuevas tecnologías, ya que otrora el acosador esperaba en la puerta de su domicilio o en la salida de su trabajo a la víctima, siendo hoy posible acecharla mediante GPS, hostigarla mediante mensajes automatizados o inmiscuirse en la intimidad de su teléfono celular[175].

En cuanto a los antecedentes de la conducta, la vincula de forma prevalente con la violencia doméstica, si bien reconoce que se ha ido ampliando a ámbitos por fuera de ese entorno[176].

Como elemento determinante del acoso, señala que, a partir de su indefinición, se ha echado mano de sus características para poder acotarlo, siendo prevalente que la conducta sea permanente y persistente, abarcado las formas de acoso desde los intentos de contacto hasta la irrupción de ámbitos familiares, sociales y laborales de la víctima[177].

En cuanto a la definición de acoso, ABOSO, como se dijo, reconoce la dificultad de lograr una definición que abarque todas las formas conductuales, por lo que junto con otros autores también pone énfasis en la identificación de esta conducta disvaliosa en la "policromía conductual", es decir, en la serie de actos que a primera vista se manifiestan como aislados o irrelevantes, pero que en el marco de la "persistencia y permanencia" generan resultados nocivos. En todo caso, para ABOSO, a pesar de las diversas clasificaciones de *stalker* que la doctrina ha realizado, existe un hilo vinculante entre todas esas formas de acosador —sea el *after intimate-relationship stalker*, el *acquaintance stalker* o el *stranger stalker*—: "en todas estas tipologías conductuales, los *stalkers* tienen la misma finalidad de ingresar o permanecer en el círculo afectivo o social de la víctima."[178]

---

[175] ABOSO. *Derecho penal cibernético, cit.,* p. 257, n. 7.
[176] ABOSO. *Derecho penal cibernético, cit.,* p. 259.
[177] *Ídem*, p. 261.
[178] *Ídem*, p. 268.

A pesar de lo anterior, esto es, de no adoptar ni ensayar una definición de acoso, el autor argentino sí define al ciberacoso, empero, solo vinculando de forma modal al acecho propio del acoso físico con las nuevas tecnologías de la información. Así, señala que el ciberacoso "se configura cuando el autor emplea los medios informáticos para acechar a la víctima."[179] Con esto, es claro que para ABOSO el acoso —que se repite, no define— solo se identifica con el acecho o la persecución física que despliega el agente en contra de su presa u objetivo, dejando de lado cualquier entendimiento del acoso moral.

La anterior consideración se refuerza cuando se evidencia que para ABOSO el *cyberstalking* consiste en "aquellas conductas de acoso que son desarrolladas en el mundo virtual mediante el acceso indebido a los sistemas informáticos ajenos o de la propia víctima que le permite al autor realizar un seguimiento electrónico de sus movimientos habituales"[180], es decir, el ciberacoso se manifiesta como una extensión del afán de intruismo del agente.

A diferencia de la mayoría de los autores, para ABOSO, el "acoso telefónico" —llamadas constantes— es una modalidad de *cyberstalking*, denominada "*telefonterror*", lo que no deja de ser llamativo, considerando que la tecnología de muchos teléfonos es análoga y no cibernética.

Finalmente, clasifica al ciberacoso en dos categorías: en sentido estricto y en sentido amplio.

> "El primero comprende solo la persecución persistente de la víctima en el medio virtual y el uso de amenazas y coacciones. El segundo abarca toda la gama de la criminalidad informática (acceso indebido a las cuentas de correo electrónico ajenas, virus malicioso, alteración de datos o configuraciones, interceptación de comunicaciones o de datos, etc.); afectación al honor y difusión de imágenes, documentos o datos contra la voluntad del afectado."[181]

18. En el derecho vernáculo, POSADA MAYA considera que "uno de los comportamientos más lesivos en el contexto de las redes sociales actuales (Twitter, Facebook, etcétera) y foros de chat es, justamente, el acoso u hostigamiento cibernético a otros usuarios de tales medios de comunicación, bien se trate de personas naturales, grupos de personas u organizaciones públicas o privadas, con diversos propósitos criminales."[182]

De lo dicho, se puede extraer que este autor colombiano equipara las conductas de acoso y hostigamiento cibernético, considera que las víctimas pueden ser sujetos individuales o grupales y que los ataques se desarrollan solo en contextos

---

[179] ABOSO. *Derecho penal cibernético, cit.,* p. 288.
[180] ABOSO. *Derecho penal cibernético, cit.,* p. 288.
[181] *Ídem*, p. 289.
[182] POSADA MAYA. *Los cibercrímenes, cit.,* p. 153.

de redes sociales o foros de chats. Adicionalmente, POSADA MAYA no solo equipara el acoso y el hostigamiento cibernético, sino que considera que el acoso y hostigamiento cibernético puede presentarse en diversas modalidades: *Stalking* (hostigamiento), *mobbing* (acoso laboral), *blockbusting* (acoso inmobiliario) y *cyberbullying* (acoso escolar)[183], con lo que de alguna manera se considera que estas conductas acosadoras son especies de un acoso u hostigamiento genérico.

De otra parte, para POSADA MAYA estas conductas son cercanas al constreñimiento ilegal en nuestro ordenamiento, atentan contra la autonomía personal y se castiga el hecho de hacer tolerar a otro un comportamiento no deseado utilizando vías de hecho[184].

Finalmente, el autor colombiano no considera que la conducta implique una relación consustancial con un comportamiento informático dañoso[185] —a pesar de admitir que en estos casos los sistemas informáticos se instrumentalizan para garantizar el anonimato—, por lo que podría afirmarse que no deba ser considerado cibercrimen y por ello no fue tipificado por el legislador colombiano en la Ley 1273 de 2009, cuyo objeto de protección es la información y los datos.

D. Tipologías conductuales

Las diversas tipologías o modalidades de acoso y de ciberacoso suponen conductas que las legislaciones y la doctrina han reseñado con el objeto de concretar la forma en que estos actos son ejecutados. Si bien no todas las legislaciones adoptan una técnica legislativa que enliste estas tipologías o modalidades, muchas otras sí lo han hecho con el fin de salvaguardar el principio de tipicidad estricta o de determinación de la conducta.

En todo caso, en relación con el tema de investigación, debe afirmarse que las tipologías de acoso y de ciberacoso las más de las veces se superponen y se identifican, en especial en los casos en que el acosador ha optado por diversos medios de acoso, tanto físico-tradicionales como cibernéticos —lo que acontece con mucha frecuencia en los contextos de violencia doméstica y de género— por lo que no es un elemento fundamental para lograr una conceptualización autónoma de las diversas modalidades de acoso u hostigamiento.

No obstante, hay tipologías o modalidades que son propias del acoso tradicional físico, mientras que hay otras tipologías que son exclusivas del ciberacoso.

Así mismo, es importante anotar que muchas de estas tipologías podrían adecuarse a otros tipos penales o podrían considerarse como actos inocuos,

[183] POSADA MAYA. *Los cibercrímenes, cit.,* p. 154.
[184] POSADA MAYA. *Los cibercrímenes, cit.,* p. 155.
[185] POSADA MAYA. *Ob. Cit.,* p. 155.

bagatela o carentes de lesividad material para ser considerados como relevantes para el derecho penal. Sobre lo primero, surge entonces el debate técnico-legislativo sobre la necesidad de tipificación de la conducta en primer lugar, o sobre si ella debe ser consagrada con una fórmula subsidiaria que salvaguarde el principio de no doble incriminación, o si, por el contrario, si a pesar de las críticas de violación del *non bis in ídem*, deban esas conductas concursar materialmente. Sobre lo segundo, resulta relevante la adopción conceptual que se tenga del acoso y del ciberacoso, que como arriba se acaba de reseñar, da vital importancia a que los actos que son aislados y que por ese mismo aislamiento pueden ser considerados irrelevantes, se tornan llamativos para el derecho penal al ser ejecutados de forma reiterada e insistente.

1. Vigilancia, persecución o búsqueda de cercanía física

Este tipo de conducta acosadora, como su nombre lo indica, es exclusiva del acoso físico, por cuanto que la acción consiste en físicamente vigilar los movimientos y perseguir en sus desplazamientos a la víctima. Esta forma de acoso es la que se adecúa con las denominaciones de "acecho" o "acoso predatorio", que nosotros adoptamos en nuestra toma de postura, ya que se hace un símil con la conducta natural de los animales que cazan a otros.

La vigilancia y la persecución son las conductas tradicionales del acoso, las cuales se ejecutan con motivaciones de poder y control, ya que el victimario busca controlar los movimientos diarios de su víctima[186].

La búsqueda de cercanía física también es una modalidad típica del acoso tradicional y se diferencia de la vigilancia y la persecución en cuanto que de forma expresa el acosador se hace notar por la víctima, al ocupar su mismo espacio de desarrollo físico-vital, aparecer en los lugares en donde normalmente se encuentra o estar ahí antes del arribo de la víctima.

La doctrina[187], de hecho, ha discutido si en la modalidad de vigilancia y persecución la víctima debe saber de la vigilancia y persecución del agente. Mientras que unos consideran que ello es necesario para concretar el resultado que algunos tipos penales exigen (la alteración de la vida cotidiana de la víctima o la generación de temor razonablemente), otros descartan este aspecto como requisito, ya que el resultado requerido no es físico, sino jurídico (de peligro).

---

[186] LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso, cit.,* p. 29.

[187] ÁLVAREZ ÁLVAREZ. *Consideraciones sobre el nuevo delito de acoso, cit.,* p. 13. Con otras referencias, LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso, cit.,* p. 29.

Con todo, debe aceptarse que la vigilancia y persecución física, y la búsqueda de cercanía física no consentida, son medios idóneos para intimidar u hostigar al sujeto pasivo.

2. Comunicación con la víctima

Esta tipología o modalidad puede predicarse tanto del acoso como del ciberacoso. Desde una perspectiva amplia, las provisiones legislativas se han referido a "establecer comunicación con la víctima", lo que puede realizarse tanto por medios tradicionales (cartas o telegramas, por ejemplo), análogos (teléfonos, fax) o cibernéticos (correo electrónico, redes sociales, chats).

Aquí la conducta consiste en el envío de comunicaciones —de forma reiterada— sin que ellas hayan sido solicitadas, aceptadas o queridas por la víctima. En este sentido, esta modalidad se constituye en la más común e idónea para intimidar u hostigar a la víctima. El recibir llamadas silenciosas, cartas, correos electrónicos o mensajes en redes sociales o grupos de chat con contenidos intimidantes o degradantes, de forma reiterada, constituyen cursos o patrones de conducta que tornan estos actos aislados como relevantes penalmente, al tener la potencialidad de generar miedo razonablemente, alterar la cotidianeidad de la víctima o en términos generales lesionar su autonomía y autodeterminación, tanto en el mundo físico como en el mundo cibernético, debiendo cambiar de domicilio, de número de teléfono y de celular, cerrar cuentas en redes sociales, cambiar sus rutas habituales o incluso no salir de su domicilio.

Tanto en la forma análoga como cibernética hay posibilidad de mantenerse en anonimato. Empero, mantenerlo en la forma análoga puede llegar a ser más complicado —por ende, más fácil de perseguir judicialmente— que en la forma cibernética. En efecto, el Internet provee una gran cantidad de servicios que protegen el anonimato, como los llamados *re-emailers*, que son servicios que borran la meta data de los mensajes electrónicos, o el simple hecho de poder crear un sinnúmero de correos electrónicos o de cuentas en redes sociales en donde la provisión de datos personales puede ser falsa y las más de las veces no es verificada por los prestadores de los servicios. Así mismo, cibercriminales con amplio conocimiento técnico y especializado pueden navegar en la *deep web* o en el Internet profundo, por medio de enrutadores que protegen y ocultan el origen de las direcciones IP desde donde los computadores operan, dificultando aún más la persecución.

En el caso de la comunicación con la víctima vía el ciberespacio, hay discusión sobre la posibilidad de la automatización de esa conducta[188]. En efecto, como se

[188] Cfr. CLOUGH. *Principles of cybercrime, cit.,* p. 376.

ha dicho, una característica propia de la cibercriminalidad es que puede ser automatizada, es decir, que una simple orden o acción del agente puede traducirse en un sinnúmero de comunicaciones, repetitivas y rápidas (por ejemplo, los *e-mails bombers*). Desde la perspectiva dogmática, se discute si esa sola acción ya supone un patrón de conducta o un curso de conducta (es decir, si se cumple con el requerimiento de que el acoso supone un conjunto de actos repetitivos). Sobre ello, no debe perderse de vista que la automatización es un rasgo distintivo de la cibercriminalidad, que se torna muy relevante, por ejemplo, en el tópico del ciberacoso, ya que lo requerido conceptualmente es que la víctima tenga que soportar reiteradas comunicaciones. En este orden de ideas, nada obstaría para considerar que existe un curso de conducta en esta situación, la cual simplemente fue facilitada por las nuevas posibilidades que la Revolución Tecnológica introdujo en nuestro medio. En nuestra toma de postura, ahondamos en mayores consideraciones para considerar este supuesto de hecho como un curso o patrón de conducta.

Otro aspecto relevante en esta tipología es que algunas provisiones legales permiten que la conducta se consume no solo con la repetitiva comunicación con la víctima, sino también con la repetitiva comunicación con personas cercanas a la víctima, con miras a establecer la relación comunicativa con el sujeto pasivo[189]. Así, el establecer repetitivamente comunicaciones con un familiar o amigo de la víctima podría consumar el delito.

También se ha tornado importante el análisis de imputación objetiva en esa modalidad. Por ello, algunos sostienen que considerando la capacidad de la víctima de bloquear contactos (por ejemplo, en redes sociales o aplicaciones de mensajería instantánea), si ello no es realizado, podríamos estar ante una situación de atipicidad de la conducta por el hecho de la víctima (consentimiento, en concreto)[190].

Finalmente, otro debate de gran envergadura en relación con la tipología de comunicación con la víctima tiene que ver con que si la comunicación tiene que estar dirigida a la víctima o si ella puede dirigirse al público en general, sin que la víctima se entere. Esta situación fue objeto de intensos debates en el caso denominado como "Jake Baker"[191] en Estados Unidos, donde el acusado —Baker— publicó en una página web varias historias ficticias en las cuales describía el secuestro, violación, tortura, mutilación y homicidio de mujeres. En una historia en particular, describió la tortura, violación y homicidio de una persona con el mismo nombre que una compañera de clases de Baker en la universidad. En otra

[189] LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso, cit.,* p. 30.
[190] ÁLVAREZ ÁLVAREZ. *Consideraciones sobre el nuevo delito de acoso, cit.,* p. 14.
[191] Cfr. CLOUGH. *Principles of cybercrime, cit.,* p. 377;

historia, publicó la dirección del domicilio de la estudiante. Así mismo, intercambió correos electrónicos con un tercero en los cuales fantaseaban sobre llevar a cabo las conductas descritas.

Este caso fue resuelto a favor de Baker, ya que se consideró que no hubo comunicación con la víctima, que ella nunca se dio por enterada del asunto y que de alguna manera las historias de Baker estaban protegidas por la libertad de expresión. La Unión Americana de Libertades Civiles (ACLU, por sus siglas en inglés) llegó a afirmar sobre el caso: "No hay lesión inmediata por la expresión del deseo de cometer un crimen." [192] Con ello, se concluyó que el discurso de Baker era discurso protegido por la Constitución.

Este debate se compone de dos elementos. De un lado, que la comunicación sea dirigida a la víctima; y de otro, que la comunicación amenazante o intimidante no esté protegida por el principio de libertad de expresión. En nuestra opinión, hay un tercer elemento importante para tener en cuenta: el principio de acto. Más allá de las horribles descripciones realizadas por Baker, sus escritos eran ficcionales, nunca ejecutó esos actos y ni siquiera ejecutó el acto comunicativo en relación con la presunta víctima. Empero, otros sostienen que el solo utilizar el nombre de la víctima ya implica una comunicación dirigida a ella, así ella no se haya percatado de la misma, lo que no tendría ninguna incidencia si la técnica legislativa adoptada no exige un resultado físico, sino uno jurídico de peligro[193].

3. Publicación de información sobre la víctima y suplantación

Esta tipología es posible tanto en el acoso físico como en el ciberacoso. Empero, debe afirmarse que existe prevalencia de la modalidad en el ciberacoso, en especial por dos razones. La primera porque la publicación en medios tradicionales (como diarios y revistas) conlleva un filtro, normalmente profesional, que implica que la acción de publicación de información sobre la víctima se va a ver controlada en esos filtros, mientras que en el Internet estos filtros son inexistentes, pudiendo publicarse cualquier tipo de información sin que los proveedores de servicios o los alojamientos web filtren lo que puede ser publicado de lo que no. Y, en segundo lugar, porque la Revolución Tecnológica le ha dado un nuevo significado y alcance a la expresión "medio masivo de comunicación". Si bien la prensa y demás medios tradicionales son considerados "masivos", no debe perderse de vista que su alcance es limitado, las más de las veces a circuitos locales o máximo nacionales de circulación. Contrario a ello, Internet sí llega de forma rápida y accesible a un público masivo, ya que trasciende fronteras y

[192] ELLISON, Louise; AKDENIZ, Yaman. "Cyberstalking: The regulation of harassment on the Internet", en *Criminal Law Review*, diciembre de 1998, p. 33. (*Trad. del Aut.*).
[193] Cfr. CLOUGH. *Principles of cybercrime, cit.,* pp. 378-379.

alcanza a abarcar a gran parte del globo. En este orden de ideas, los casos que se han resuelto en el derecho comparado tienen mayor relación de prevalencia con el ciberacoso que con el acoso tradicional.

La modalidad conductual consiste en publicar información personal de la víctima para que el público masivo acceda a esa información y ejecute actos de hostigamiento o de intimidación en contra de ella. El típico caso, resuelto por lo demás en varias jurisdicciones[194], supone que una expareja o sujeto rechazado por la víctima publica su información personal, sus fotografías modificadas por medio de fotomontajes sexuales, solicitando ser contactada para regalar o prestar servicios sexuales. Reglón seguido, la víctima es contactada y hostigada por una multitud de personas buscando sus servicios.

Otro caso similar implicó que la publicación de la información de la víctima no era tanto para prestar servicios sexuales, sino que se solicitaba que la víctima fuera violada, al ser esa supuestamente una fantasía suya. Otro caso más supuso que el agente publicó información de la víctima, en concreto los nombres de sus hijos y fotos de ellos tomadas de forma subrepticia, con sus números de contacto, motivando al público a contactarlos, lo que resultó en diversas llamadas de pedófilos solicitando actos sexuales de los menores[195].

Estos casos ilustran dos elementos importantes. De un lado, puede existir —y así sucede las más de las veces— una suplantación de la víctima[196], lo que en nuestro medio constituiría una falsedad personal. Aquí cobraría relevancia, una vez más, el debate concursal o subsidiario de la conducta, lo que debe ser acometido por una técnica legislativa que respete los principios rectores de *non bis in ídem* y de concurso efectivo de conductas punibles. De otro lado, en segundo lugar, también existe cercanía con esta modalidad y el tipo penal de violación de datos personales, ya que se está dando un uso inadecuado a los datos personales de la víctima. Empero, en nuestro medio se debe descartar sin discusión una subsunción en el tipo penal de violación de datos personales, ya que él comporta un elemento normativo de provecho propio o de un tercero, el que puede no existir en los casos de ciberacoso. En efecto, puede que la motivación del agente no sea

[194] PITTARO. "Cyberstalking", *cit.,* pp. 282 y ss.; CLOUGH. *Principles of cybercrime, cit.,* p. 380; HOFFMEISTER. "Legislative reactions", *cit.,* p. 189.

[195] Cfr. CLOUGH. *Principles of cybercrime, cit.,* p. 380.

[196] HOFFMEISTER ("Legislative reactions", *cit.,* p. 188) señala que, a diferencia de las suplantaciones tradicionales, la suplantación *online* carece de un componente motivacional económico. De esta forma, la suplantación no busca la defraudación económica sino lesionar a la víctima por medio del hostigamiento o del avergonzamiento.

la obtención de ningún beneficio, económico o de otra naturaleza, sino simplemente ejercer poder, control o satisfacer una venganza privada[197].

Con ello, se quiere resaltar que, si en algunos casos la conducta se torna atípica de cara a la violación de datos personales, ella puede no serla de cara al ciberacoso, siempre que se satisfagan con los requisitos de esa conducta, que son, de la forma más general, que ella consista en un conjunto de conductas repetitivas que buscan intimidar u hostigar a la víctima.

Otro ejemplo que puede encuadrarse en esta modalidad es aquel en el que el agente publica información de la víctima o la suplanta, haciendo manifestaciones que rayan con las sensibilidades de la población en general, produciendo que terceros intimiden a la víctima. Por ejemplo, como cuando se publica que la víctima está de acuerdo con el maltrato animal o con el abuso infantil, recibiendo entonces llamadas intimidantes por supuestamente defender posiciones indefendibles.

En este orden de ideas, se vislumbra como esta modalidad conlleva una intimidación u hostigamiento ejecutada por terceros, de donde vuelve a surgir el debate sobre la satisfacción del requisito del curso de conducta o del conjunto de actos repetitivos. En este caso, la automatización no juega un papel prevalente, ya que el acto del agente no ha sido programado cibernéticamente para reproducirse, sino que la reproducción de este se da partir de la publicación de información sensible o la suplantación en relación con temas llamativos para terceros, logrando convocarlos a la campaña de acoso o instrumentalizándolos para ese fin.

Desde la perspectiva dogmática, esta situación será una de autoría accesoria o de autoría mediata. La primera si la acción del agente se junta con la acción de terceros, sin acuerdo previo, ejecutando el acto; la segunda si se ha instrumentalizado a los terceros, que se embarcan en la ejecución de sus conductas sin saber que están intimidando u hostigando al tercero a partir de la acción engañosa del victimario. Siendo ello así, es posible zanjar el requisito de la multiplicidad de actos, el cual se vería satisfecho, ya que nada es óbice para que el curso de conducta o conjunto de actos se tornen criminales ya sea porque los ejecutó personalmente el autor (autoría directa o inmediata) o porque, como

---

[197] SUÁREZ SÁNCHEZ. *Manual de delito informático en Colombia, cit.,* p. 313: "Si el ánimo del sujeto activo es distinto al de lograr un beneficio, por ejemplo, satisfacer una venganza, el delito no se tipifica, *ya que el vengador suele estar inmerso en sentimientos de odio y rencor*, los que no generan beneficio o utilidad. Como ya se destacó, este elemento normativo da lugar a la impunidad en algunos casos, porque si el sujeto realiza cualquiera de las plurales conductas sin tener el propósito de aprovechamiento y sin lograr el mismo después de la ejecución, sino llevado por estímulos diferentes o empujado por el solo propósito de violar la privacidad de los datos o los códigos personales, la conducta es atípica." (Cursiva del original).

sucede en otros delitos de medios abiertos, instrumentalizó mediante error a terceros para la ejecución repetitiva y plural de la conducta[198].

4. Vigilancia electrónica

Así como la vigilancia física es exclusiva del acoso físico tradicional, la vigilancia electrónica es exclusiva del acoso cibernético. Empero, en ambos casos, en relación con los contextos que se motivan mediante la relación de poder y el ejercicio del control, el conocimiento que el victimario tiene sobre la víctima y la información que sobre ella y su vida puede recaudar, son insumos determinantes para ejecutar la intimidación y el hostigamiento.

Un aspecto social importante, que de nuevo confirma los profundos cambios sociales generados por la Revolución Tecnológica en nuestros medios, es que mucha de la información que utiliza el ciberacosador para realizar la intimidación o el hostigamiento ha sido publicada voluntariamente por la víctima, lo que genera debates acerca de la asunción del riesgo, que a nuestro juicio, son inadmisibles, ya que la publicación de información del usuario digital hace parte de su libre desarrollo de la personalidad en el ciberespacio. Otro asunto será el no adoptar medidas de prevención, como configurar la cuenta como privada.

Con todo, la información que sea obtenida por el ciberacosador mediante métodos tecnológicos puede ser utilizada para ahondar en las demás tipologías o conductas de ciberacoso o de acoso tradicional. De un lado, servirá para vigilar o perseguir físicamente a la víctima. De otro, es información relevante para construir mensajes comunicativos más intimidantes y hostigadores que lleven a la víctima a coartar su autodeterminación.

En el contexto de la violencia doméstica y de género, los métodos de vigilancia electrónica pueden ser de baja o alta tecnología (*low-tech method* o *hi-tech method*)[199]. Dentro de la primera categoría está el acceder a los repositorios digitales de la víctima, para ejercer control o dominio sobre sus actividades. Dentro de la segunda categoría hay mecanismos más complejos y técnicos, como la instalación de *key loggers* (un programa que envía al dispositivo del agente las teclas presionadas por la víctima en su propio dispositivo) o *screen loggers* (un programa que envía al dispositivo del agente todas las actividades realizadas por la víctima en su propio dispositivo) en los dispositivos electrónicos de la víctima, o la instalación de cámaras ocultas o de sistemas de GPS para ubicarla en todo momento.

---

[198] Con comentarios sobre el problema de la autoría mediata en estos casos, cfr. LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso, cit.,* pp. 31, 37-40; ÁLVAREZ ÁLVAREZ. *Consideraciones sobre el nuevo delito de acoso, cit.,* p. 14.

[199] Cfr. NAVARRO. "Cyberabuse and cyberstalking", *cit.,* pp.127-128.

Según CLOUGH[200], la mayoría de los ordenamientos jurídicos no consideraran la vigilancia electrónica como constitutiva de ciberacoso a menos que la víctima esté consciente de la vigilancia y que se combine con otras conductas de acoso o de ciberacoso. Este aspecto del conocimiento de la víctima vuelve a relacionarse con el debate sobre si lo requerido es un resultado en el mundo físico —el miedo de la víctima— o un resultado jurídico de peligro —que la acción tenga la potencialidad de generar miedo en la víctima—.

En todo caso, parece ser acertado considerar que la mera vigilancia electrónica no supone ciberacoso, a menos que ella vaya de la mano de otras conductas repetitivas que tengan por objeto intimidar u hostigar, ya que la sola acción de vigilancia, conocida o no por la víctima, estará más cerca de conductas de intruismo informático (como el acceso abusivo a un sistema informático) o de interceptación de comunicaciones o de datos informático, o incluso de uso de *software* malicioso.

5. Ataque a los dispositivos de la víctima

Esta modalidad exclusiva de ciberacoso es recogida por la doctrina[201], señalando que es posible que el ciberacosador intervenga en los dispositivos electrónicos de la víctima con miras a ejercer intimidación o para vigilarla electrónicamente. Por ejemplo, puede que la víctima reciba un mensaje que rece “te voy a atrapar” y acto seguido la unidad de CD de su computador se abra y cierre varias veces.

Sin embargo, este tipo de conducta es más cercana al intruismo informático y al daño informático. Así, puede generar debates en el ámbito concursal y de prohibición de doble incriminación.

E. Teorías etiológicas prevalentes

Realizada la reseña doctrinal sobre los diversos conceptos de acoso en línea y acoso fuera de línea, y también sobre las diversas tipologías conductuales de esos actos lesivos, es relevante revisar las diversas teorías criminológicas que buscan explicar las causas de los comportamientos desviados bajo estudio.

Determinar con exactitud las causas de un comportamiento desviado es una tarea no solo imposible, sino inadecuada. Como se ha reconocido, la criminología no es una ciencia aplicativa o exacta, sino causal-explica[202]. Incluso, es tendencia actual no considerar a la criminología como “ciencia” en lo absoluto, sino en un campo multidisciplinario que estudia el fenómeno de la desviación criminal y la reacción

[200] CLOUGH. *Principles of cybercrime, cit.,* p. 387.
[201] CLOUGH. *Principles of cybercrime, cit.,* p. 384.
[202] REYES ECHANDÍA, Alfonso. *Criminología*, 8ª ed., Bogotá, Temis, 2003, p. 1.

social a ello[203], esté o no tipificado en la ley penal la conducta desviada[204]. Por lo anterior, no es posible sostener que existen respuestas únicas y correctas a la explicación etiológica de los fenómenos criminales, sino a lo sumo existirán explicaciones plausibles que sirvan de guía para la implementación de políticas públicas de prevención general y especial.

Así, la criminología, como disciplina social, aportará sus criterios con el fin de encauzar una conceptualización adecuada del fenómeno criminal bajo estudio. De esta forma, a diferencia de las tipologías conductuales —que son más orientadoras—, el estudio etiológico puede dar luces sobre los campos conceptuales que componen al acoso, al hostigamiento y a sus versiones cibernéticas. Bajo esta egida, emprendemos esta reseña criminológica.

1. Teoría psicológica

REYES ECHANDÍA señala que "todo hecho delictuoso, como todo comportamiento humano, es el resultado de una serie de operaciones psíquicas que se exteriorizan mediante movimientos corporales, con lo que es necesario admitir la presencia de un componente psíquico en cualquier conducta antisocial."[205] Con ello, se quiere decir que el elemento de sanidad/enfermedad mental es relevante en la explicación del delito en general.

Sin embargo, incluso hoy, ello no es tan claro. PITTARO reconoce que se ha esparcido como un mito que los ciberacosadores cometen este tipo de conductas por sufrir de algún tipo de desorden mental[206]. En efecto, la conexión entre crimen y enfermedad mental no es muy clara, empezando porque las definiciones de "crimen" y de "enfermedad mental" no son pacíficas en la doctrina científica. Más allá, la prevalencia de determinados comportamientos entre los diversos grupos poblacionales —en este caso, entre los enfermos mentales y los sanos mentales— no se soporta en una evidencia conclusiva y, por el contrario, son numerosos los cuestionamientos que pueden elevarse para criticar una posición que sostenga que determinados comportamientos son prevalentes en determinadas poblaciones, como en este caso sería afirmar que el ciberacoso es prevalente en los sujetos con desordenes a nivel psiquiátrico.

Así, por ejemplo, NEWBURN[207] señala que la evidencia demuestra que la mayoría de enfermos mentales no son peligrosos; los tipos de ofensas cometidos por los enfermos mentales son ampliamente similares a los tipos de ofensas cometidos

[203] NEWBURN, Tim. *Criminology*, 2ª ed., London, Routledge, 2013, p. 5.
[204] PÉREZ KASPARIAN, Sara. *Manual de criminología*, Ciudad de México, Porrúa, 2014, p. 3.
[205] REYES ECHANDÍA. *Criminología, cit.,* p. 66.
[206] PITTARO. "Cyberstalking", *cit.,* p. 287.
[207] NEWBURN. *Criminology, cit.,* pp. 870-873.

por la población no enferma; que los estudios demuestran que las personas sanas cometen más delitos que las personas enfermas y que los enfermos mentales dados de alta en los hospitales reinciden menos en actividades criminales que los que salen de las prisiones, por lo que concluye que este tópico debe ser abordado con demasiada cautela, no perdiendo de vista que existe una forma de victimización en contra de la población que sufre enfermedades mentales.

Empero, algunos autores[208] sostienen que existe una prevalencia de enfermedades mentales en los ciberacosadores, en especial, un tipo de desorden delirante erotomaníaco denominado Síndrome de Clerambault, el cual es utilizado para explicar el comportamiento de los sujetos que en realidad creen que se encuentran inmersos en una relación íntima con otra persona, en este caso, la víctima. Lo anterior parece ser una tipología criminal que busca encuadrar al acosador obsesivo que persigue a celebridades. Sin embargo, el ciberacosador no siempre se comporta de dicha manera, en cuanto que las más de las veces es un sujeto solitario que ataca sin moverse de su terminal electrónica, es decir, sin querer cercanía física o amorosa con la víctima.

2. Teoría del aprendizaje social

Las teorías del aprendizaje llegan al campo criminológico a partir del trabajo de sociólogos y psicólogos. Respecto de los primeros, el trabajo de SUTHERLAND (la teoría de la asociación diferencial) se comporta como el más relevante. Respecto de los segundos, la teoría del aprendizaje operativo de SKINNER —inspirado en los experimentos que con perros hizo PAVLOV finales del siglo XIX y principios del siglo XX— y la teoría concreta del aprendizaje social por observación de BANDURA, se manifiestan como los más icónicos.

Según la teoría general del aprendizaje social

> "los comportamientos humanos proceden del aprendizaje, bien de manera directa, bien mediante la observación que se hace de la conducta de los demás, sin que ello signifique simple imitación o remedo. El aprendizaje, además, no es tan sencillo pues implica adquirir modelos, retenerlos o almacenarlos, y aceptarlos, apropiarlos y reproducirlos."[209]

Dos conceptos medulares de las teorías del aprendizaje son el condicionamiento clásico (acuñado por PAVLOV) y el condicionamiento operativo (sostenido por SKINNER)[210]. Por medio de estos conceptos se pretende explicar cómo el comportamiento humano es consecuencia de la interacción del individuo con el mundo que lo rodea, es decir, nos comportamos —conforme a derecho o

---

[208] Cfr. PITTARO. "Cyberstalking", *cit.,* pp. 287-288.

[209] PÉREZ PINZÓN, Álvaro Orlando; PÉREZ CASTRO, Brenda Johanna. *Curso de criminología,* 7ª ed., Bogotá, Universidad Externado de Colombia, 2006, p. 77.

[210] NEWBURN. *Criminology, cit.,* pp. 151-156.

criminalmente— a partir de nuestro aprendizaje social. El condicionamiento clásico sostiene que es posible provocar un comportamiento a partir de la vinculación *a priori* de un estímulo con una recompensa. Fue precisamente a partir del experimento con los perros que PAVLOV descubrió este tipo de conductismo comportamental. En ese experimento, PAVLOV notó que siempre que les suministraba comida a sus perros, ellos babeaban. Seguidamente, siempre que les suministraba a sus perros comida, hacía sonar una campana. La acción fue repetida tantas veces que, después de un tiempo, sin presentar ningún tipo de comida, solo con hacer sonar la campana, los perros empezaban a babear.

El condicionamiento operativo se diferencia del clásico en que el conductismo comportamental también es posible por medio del refuerzo positivo o negativo *a posteriori*. SKINNER probó su concepto por medio de la experimentación con ratas. En un experimento, creó una caja en la que encerró a una rata. Ahí, sin comida, la rata podría realizar ciertos actos, unos que le recompensaban positivamente con comida y otros que le recompensaban negativamente con choques eléctricos. A partir del aprendizaje, la rata logró dilucidar la dinámica y empezó solo ejecutar actos con refuerzo positivo y a evitar actos cuyas consecuencias sabía que eran negativas.

Finalmente, BANDURA[211] también llevó a cabo un experimento con el que acreditó la validez de su teoría del aprendizaje social por observación. Su experimento, denominado como del "muñeco Bobo" o *Bobo doll experiment*, implicaba que se dividirían a un grupo de niños en dos grupos. Un primer grupo de niños fue dispuesto para observar como un adulto golpeaba y era agresivo con el muñeco Bobo, que era uno de aquellos juguetes que son de goma inflable, tienen diseño de un payaso y una forma de balón en la parte inferior, por lo que se balancean y rebotan. El segundo grupo de niños fue dispuesto también a ver al adulto, pero sin que él tocara al muñeco Bobo. Después, los dos grupos fueron introducidos a un salón de juegos y juguetes en donde se encontraba el muñeco Bobo. Solo los niños del primer grupo repitieron e incrementaron los golpes en contra del muñeco, las cuales habían visto previamente ser ejecutadas por el "modelo" (concepto de Bandura que hace referencia al "modelo a seguir" o al "modelo influenciador"). Con ello, concluye que determinados comportamientos humanos devienen del aprendizaje social que realizan a través de la observación de modelos de conducta, como son los padres, los pares, los famosos, etc.

Algunos autores[212] sostienen que la teoría del aprendizaje social es válida para explicar la etiología del ciberacoso. Acorde con ello, si una víctima responde al curso de conducta intimidante u hostigador del ciberacosador, entonces el

[211] PÉREZ KASPARIAN. *Manual de criminología, cit.,* pp. 48-49.
[212] Cfr. PITTARO. "Cyberstalking", *cit.,* p. 288.

ciberacosador habrá recibido un refuerzo positivo para seguir ejecutando la conducta, ya que logró una reacción en su víctima, sea ella positiva o negativa. PITTARO refiere que este tipo de razonamiento también aplica a los exhibicionistas sexuales, que al mostrar sus genitales en público y generar shock o rechazo de las víctimas, se verá reforzado positivamente a volverlo a hacer, pues esa era la reacción que esperaba. En este sentido, lo recomendable frente a los ciberacosadores es ignorarlos, no empezar una discusión directa y en vez de ello, denunciarlos o reportarlos.

3. Teoría de la elección racional y teoría de las actividades rutinarias

La teoría de la elección racional es una manifestación del análisis económico del derecho y la introducción del concepto de *homo economicus*, es decir, del sujeto racional que balancea los beneficios (utilidades) o riesgos (pérdidas) que una acción u omisión le pueden generar. Este tipo de razonamiento fue popularizado en 1968 por el economista ganador del Premio Nobel Gary Becker, quien sostuvo que los individuos cometerán ofensas criminales si la utilidad esperada de hacerlo es positiva, y no lo harán si es negativa. Con ello, la teoría de la elección racional sostiene que los criminales ejecutaran sus actos desviados cuando los beneficios de la conducta pesen más que los riesgos o las pérdidas por ejecutarla[213].

En este sentido, esta teoría deja de lado las ideas que sostienen que el crimen es *reacción* a una interacción social (aprendizaje social, etiquetamiento, anomia), siendo más bien una *acción*, o mejor, una *elección* del sujeto frente a los riesgos y beneficios de la conducta. “En resumen, el divergente, ante la ocasión que le surge para delinquir, y guiado por su exclusivo interés, sopesa frutos o productos de su acto y peligro de ser sorprendido o capturado, y *escoge*.”[214]

Es precisamente por este elemento de la “oportunidad para delinquir” que la teoría de la elección racional puede integrarse con la teoría de las actividades rutinarias. Según esta teoría, presentada primigeniamente por FELSON y COHEN en 1979, el enfoque del estudio criminológico debe estar en el evento criminal y no en el ofensor[215]. Sus postulados pretendían explicar por qué en la época de postguerra los crímenes en Estados Unidos estaban aumentando —en especial el hurto de viviendas— si los índices que normalmente se relacionan con el crimen estaban disminuyendo (la pobreza, el desempleo, la falta de educación).

---

[213] NEWBURN. *Criminology, cit.,* p. 287.
[214] PÉREZ PINZÓN, PÉREZ CASTRO. *Curso de criminología, cit.,* p. 97.
[215] NEWBURN. *Criminology, cit.,* p. 292.

La explicación propuesta indicaba que el cambio estructural de las actividades rutinarias culturales y diarias de la población tenía incidencia en el crimen, cuando tres elementos concurrían en el tiempo y en el espacio[216]:

i. La presencia de un agresor motivado.

ii. La existencia de una víctima adecuada.

iii. La ausencia de un vigilante capacitado.

De concurrir estos tres elementos, la posibilidad de ejecución de delito aumentaba, mientras que con que no existiera alguno de los tres, la posibilidad de ejecución disminuía.

En relación con el ciberacoso, es palmario que los cibercriminales sopesan los riesgos que corren al ejecutar la conducta y de ser descubiertos o capturados. Así, al verificar que sus acciones tienen lugar en el ciberespacio, que es un territorio en cierta medida anómico, que no existen guardianes capacitados para perseguirlos, que pueden esconder sus actos bajo el manto de anonimato, que hay un déficit de leyes que haga posible su persecución cuando están distantes geográficamente y que sus víctimas carecen de herramientas de defensa, entonces proceden a la ejecución de la conducta.

> "En otras palabras, el ciberacosador, como un ofensor motivado, buscará y hostigará a una víctima (un objetivo adecuado) en la ausencia de guardianes capacitados, lo que, en esta situación, se da a través del anonimato del Internet, lo cual provee protección en contra de la detección. (…) las mujeres pueden ser objetivos adecuados porque la victimización del ciberacoso aún no ha sido tomada en serio por la sociedad ni ha recibido la atención que merece del sistema judicial criminal."[217]

En este orden de ideas, no existe una prevención real que desmotive la acción criminal del ciberacosador, ya que la balanza en la que sopesa el riesgo y el beneficio siempre está inclinada hacia el beneficio, considerando que el riesgo de detención es bajo y, aun revelando la identidad del agente, el riesgo de ser capturado, judicializado y condenado también es bajo, haciendo entonces del ciberacoso una conducta atractiva para los cibercriminales.

Sin embargo, no debe perderse de vista que la teoría de las actividades rutinarias no ha estado exenta de críticas en relación con su aplicación a los cibercrímenes.

---

[216] PÉREZ PINZÓN, PÉREZ CASTRO. *Curso de criminología, cit.,* pp. 158-159; NEWBURN. *Criminology, cit.,* p. 293.

[217] PITTARO. "Cyberstalking", *cit.,* pp. 288-289. *(Trad. del Aut.).*

En efecto, se han presentado tres críticas concretas[218]: primero, que es cuestionable la exigencia que hace la teoría en cuanto que debe existir una convergencia "de espacio y tiempo" de sus tres elementos, ya que precisamente una de las características predominantes de la cibercriminalidad es que el ciberespacio permite la relatividad de que el espacio y el tiempo converjan.

En segundo lugar, la ausencia de un guardián capacitado puede variar de agresor a agresor, ya que la efectividad de la protección del guardián dependerá de las habilidades cibernéticas e informáticas del agente.

Finalmente, dado que los guardianes en el ciberespacio son invisibles (ya que mientras que en el mundo físico se puede percibir sensorialmente la existencia de una cámara de seguridad, de una valla alta o de un policía, en el ciberespacio las protecciones no se perciben a primera vista, como un determinado programa fuerte de *firewall*), entonces se torna difícil para el potencial cibercriminal sopesar los costos de ejecutar o no la conducta, considerando que pueden no tener certeza acerca de la intensidad de la seguridad presentada.

En nuestra opinión, así como lo han sostenido diversos autores[219], la teoría de las actividades rutinarias es apta para explicar el fenómeno del acoso en línea, en especial del acoso de hostigamiento moral. Así, ensayaremos en nuestra toma de postura sendas respuestas a las críticas presentadas por KREMLING y SHARP PARKER.

[218] KREMLING, SHARP PARKER. *Cyberspace, cybersecurity and cybercrime, cit.,* p. 165.
[219] Cfr. PITTARO. "Cyberstalking", *cit.,* pp. 288-289.

CAPÍTULO TERCERO

La delimitación entre los diversos tipos de acoso y hostigamiento (toma de postura sobre la autonomía social del acoso moral como cibercrimen en el derecho penal)

I. Elementos comunes y disimiles en los tipos de acoso

A. Introducción

Es indudable que, a partir de la reseña doctrinal realizada, deba llegarse a la conclusión de que no hay claridad sobre el concepto de acoso u hostigamiento, ni de ciberacoso o ciberhostigamiento, ni sobre la autonomía o dependencia de éstos últimos respecto de aquellos. Con todo, nuestro estudio nos ha permitido llegar a diversas conclusiones acerca de la naturaleza jurídica y criminológica de estos actos desviados, arrojando como primera conclusión que el ciberacoso es una forma de ciberviolencia y de ciberabuso, de la misma forma que el acoso es una forma de violencia y de abuso. Es decir, en los términos más generales, todo acoso y todo ciberacoso se manifiestan como conductas lesivas de bienes jurídicos personalísimos, consistentes en actos abusivos y violentos que oprobian a las personas en su libertad y autonomía.

Sobre este punto, podría admitirse que hay poca discusión en la doctrina[220]. Es partir de aquí que cada autor presenta su concepto y cada ordenamiento jurídico aplica una técnica legislativa —en los casos que lo han hecho, situación que no se ha dado en Colombia de forma integral— para gestionar estos riesgos antijurídicos.

El repaso conceptual realizado ha arrojado acepciones que integran fines sexuales o afectivos a la conducta acosadora/ciberacosadora[221]; otros, lo han identificado con una "obsesión", con lo que, si bien no necesariamente hay una vinculación con alguna enfermedad, sí se trasmite esa impresión, en cuanto que la obsesión implica una perturbación anímica de fijación con un objeto[222]. Incluso, para algunos, debe existir una relación afectiva previa, es decir, deben conocerse los sujetos[223]. Para otros, la conceptualización pasa por vincularlos a un género específico, como formas de "ciberterrorismo"[224] o de "*cyberbullying*"[225]. Para la mayoría, el acento está en la intención (de amenazar, intimidar, hostigar, obtener favores sexuales, etc.)

VILLACAMPA ESTIARTE[226] y ALONSO DE ESCAMILLA[227], además, también buscan lograr su conceptualización revisando los géneros de acoso psicológico y

---

[220] Cfr. CRISAFI, MULLINS, JASINSKI. "The rise of the virtual predator", *cit.,* pp.99, 112. NAVARRO. "Cyberabuse and cyberstalking", *cit.,* p. 125.
[221] Así, ABOSO (cfr. *supra*, n. 178).
[222] Así, MELOY y GOTHARD (cfr. *supra,* n. 96); también ALONSO DE ESCAMILLA (cfr. n 168).
[223] Por ejemplo, ROYAKKERS (cfr. *supra*, n. 103) y NAVARRO (cfr. *supra*, n. 133).
[224] En este sentido, MISHRA y MISHRA (cfr. *supra*, n. 139).
[225] Así lo sostiene KIEL (cfr. *supra*, n. 146).
[226] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* pp. 42-46.

de acoso moral. Por acoso psicológico entienden aquellas conductas reiterativas e intrusivas que generan un desequilibrio emocional en la víctima, mientras que por acoso moral se refieren a aquellas conductas reiterativas e intrusivas que generan humillación, degradación y envilecimiento en la víctima. Mientras que el *stalking* haría parte del acoso psicológico, los demás tipos de acoso —sexual, *mobbing*, *blockbusting* y *bullying*— serían formas de acoso moral.

Tenemos para nosotros que este es un buen punto de partida para ensayar una conceptualización de acoso y de ciberacoso[228]. Lo anterior por cuanto se nos presentan categorías que implican una sistematización, incluso de género a especie, lo que dará a cada espacio sus características comunes y disímiles; y es que nuestra posición es defender una conceptualización de los diversos tipos de acoso desde la perspectiva de sus elementos independientes (que los diferencian) y sus elementos dependientes (que los agrupan o acercan), para finalmente poder hablar de "acoso" frente a cada uno de ellos.

Esta posición nos resulta como la única compatible con el objetivo de lograr un concepto prejurídico de acoso y de ciberacoso que sirva para la posterior estrategia legislativa y preventiva, considerando que aquellas posiciones reseñadas y acabadas de recordar por parte de varios autores nos parecen insuficientes y deficientes, teniendo en cuenta que al vincularse con elementos concretos (intención afectiva o sexual, exparejas, enfermedad obsesiva, formas específicas de otros fenómenos), en donde hay confusiones de sistematización, terminan por excluir fenómenos cercanos y acercar fenómenos lejanos.

Así, valoramos los conceptos de acoso psicológico y acoso moral, empero, nos alejamos de la forma en que VILLACAMPA ESTIARTE y ALONSO DE ESCAMILLA los abordan. En este orden de ideas, tenemos para nosotros que todo acoso es *acoso psicológico*, pues este resultado o peligro se concreta o se cierne sobre toda víctima que de forma repetitiva e intrusiva ve su ámbito vital de libertad menguado, al existir una ruptura entre la relación de paridad y sana distancia que debe existir entre todos los asociados, en el mundo físico o en el mundo virtual. Por lo anterior, no contraponemos el acoso moral al acoso psicológico, pues creemos que el acoso moral (esto es, repetitiva e intrusivamente humillar, degradar y envilecer a la víctima) también comporta efectos psicológicos sobre ella. En este sentido, recuérdese los lamentables casos de adolescentes que a partir del acoso moral de sus pares (*bullying*, matoneo o acoso escolar) o de

---

[227] ALONSO DE ESCAMILLA. "El delito de stalking como nueva forma de acoso", *cit.,* p. 222.

[228] A partir de este punto, emplearemos exclusivamente la palabra acoso o ciberacoso hasta que abordemos el punto en el cual introducimos nuestro entendimiento del hostigamiento y ciberhostigamiento.

terceros (*harassment*, hostigamiento o acoso moral estricto) sufrieron tal desequilibro emocional que decidieron quitarse la vida[229].

Así las cosas, dados los potenciales resultados o peligros lesivos para sendos bienes jurídicos (de la libertad y la autonomía a la salud mental y la vida), el objeto de la sanción jurídica (penal, administrativa o civil) es el acoso psicológico, el cual se desdobla en diversas formas, las cuales tienen todas elementos comunes (el primero: el riesgo psicológico para la víctima), pero también elementos que los independizan.

B. Elementos comunes en los tipos de acoso

Abordando en primera medida los elementos comunes que convierten a todas estas conductas "acoso", anotamos que el primero es el riesgo psicológico para la víctima.

El segundo de ellos, pues, será el carácter repetitivo, persistente e intrusivo de la conducta. Una de las grandes dificultades de la punición o sanción jurídica en general del acoso es que los actos que lo componen pueden ser socialmente adecuados o pueden ser inocuos o carentes de lesividad. Así, mal haría el derecho penal y el derecho en general en sancionar un envío de flores, el coincidir un día en un café, el colocar una gran carga de trabajo, trasmitir un piropo o el someter a una persona al ridículo frente a sus pares. Sin embargo, cuando cada uno de esos actos es *sistemático*, en el sentido de repetirse, volverse a realizar y, a pesar de la oposición del afectado, realizarse de nuevo (intrusivo), o combinarse *sistemáticamente* cada uno de ellos, entonces se puede sostener que no estamos ante actos que se adecúen a comportamientos sociales permitidos, ni que no tengan potencial lesivo, ya que se habrá constituido una *campaña*, *patrón* o *curso de conducta*, es decir, se estará *acosando* a una víctima.

En breve: todo acoso tiene potencial de riesgo psicológico para la víctima y todo acoso es repetitivo, persistente e intrusivo. De ahí que una tipología conductual de acoso no sea *per se* delito (penal, administrativo o civil), pero la repetición de una tipología conductual o la combinación de varias sí torne la conducta como relevante para el derecho penal, el derecho administrativo y el derecho de daños.

De esta forma, todos los tipos de acoso son *dependientes* de estas dos características.

C. Elementos disímiles en los tipos de acoso

[229] En Colombia, el epítome fue el caso de Sergio Urrego. En Estados Unidos, los casos han sido varios e incluso la cultura popular lo ha fijado en el pensamiento colectivo a través de exitosas series de televisión, como la aclamada y criticada *Thirteen Reasons Why* (Netflix, 2017-).

Empero, no todo acoso es igual. Si bien todos ellos pueden generar riesgo psicológico y todos comparten la sistematicidad de su ejecución continuada y persistente, no todos ellos comparten las mismas motivaciones finales ni lo que denominamos *hábitat o entorno social*. Cada tipo de acoso comporta motivaciones diferentes y hábitats o entornos sociales diversos. De hecho, es precisamente la influencia ambiental del hábitat o entorno social la que determina o indica la motivación final del agente.

El hábitat o entorno social es el ambiente en el cual la relación intersubjetiva se desarrolla, dándole unos límites materiales y referenciales respecto de los cuales los comportamientos deben desenvolverse, de acuerdo con determinada expectativa, o no deben desenvolverse, por cuando habrán desbordado aquellos límites relacionales. Así, el hábitat o entorno social es el que impone los distanciamientos adecuados entre las relaciones de paridad de los asociados. A partir de él, es posible determinar que un agente ha sobrepasado el riesgo permitido del comportamiento social para tornar su hacer en un curso de conducta punible o sancionable.

Existen tantos hábitats o entornos sociales como relaciones sociales y ámbitos de interactuación posibles. Las relaciones afectivas, las relaciones cibernéticas, las relaciones laborales, las relaciones familiares, las relaciones escolares, las relaciones de vecindad, *et alters*, son hábitats o entornos sociales que comportan límites conductuales, los cuales, al ser sobrepasados, generan situaciones de acoso que deben ser gestionadas por el derecho.

II. Tipos de acoso psicológico

En este sentido, agrupados bajo el manto genérico del acoso psicológico, se encuentran el acoso de acecho (o predatorio) y el acoso moral (u hostigamiento).

A. Acoso de acecho o predatorio

1. Acoso de acecho o predatorio estricto

El acoso predatorio, en sentido estricto, se manifiesta como la figura “clásica” de *stalking* en la cual un sujeto persigue o vigila reiterativa y persistentemente a una víctima que encuentra dicha persecución física o electrónica como intrusiva. Esta conducta no es punible ni jurídicamente sancionada en Colombia (incluso, no se

comporta como contravención policiva más allá del deber genérico de los ciudadanos de mantener la sana convivencia[230]).

El hábitat o entorno social que permite esta conducta es el de las relaciones afectivas e interpersonales, entre parejas, exparejas o conocidos, reales o imaginadas. Así, el acoso predatorio es una forma concreta de control coercitivo (en los términos señalados por NAVARRO[231]) en la cual el agente busca ejercer control sobre su pareja o expareja, o un conocido (*acquaintance stalking*), los cuales están por fuera de ese dominio o están saliendo de él.

Esta forma de acoso es típica de los casos de acecho afectivo imaginado a las celebridades. Así mismo, es típica de las formas de abuso y violencia doméstica. Lo común en estos asuntos es que existe una relación afectiva real o imaginada que motiva al autor a intrusiva y predatoriamente perseguir a la víctima para mantenerla en su control o introducirla dentro de la influencia de este.

En estos casos, no debe perderse de vista la posibilidad de que exista una obsesión clínica, lo que será un asunto que debe ser valorado desde la perspectiva científico-médica, que implicará, a partir de los estudios pertinentes, la determinación de si el agente podía o no comprender la ilicitud de su conducta o determinarse de acuerdo con dicha comprensión por causa de un trastorno mental. En dicho caso, el acto no debe ser impune, ya que, a pesar de la inimputabilidad del sujeto, debe ser destinatario de una medida de seguridad, consecuencia que también comporta las características de la sanción penal.

En el acoso predatorio las tipologías ejecutadas pueden ser físicas o cibernéticas. Como en todos los acosos, la ejecución de la conducta puede consistir en la repetición de una de ellas o en la combinación de varias. Este tipo de acoso o acecho se concentra en la persecución de los movimientos de la víctima, con el fin de ejercer control sobre ella, sea mediante la amenaza o la intimidación. Así, la motivación del autor es vigilar, amenazar o intimidar para controlar. En este sentido, se pueden desplegar tipologías conductuales de persecución física, vigilancia física, búsqueda de cercanía física, comunicación reiterada con la víctima con contenido intrusivo, amenazante o intimidante, o vigilancia electrónica.

Como lo señala NAVARRO, existen diversos tipos de persecución electrónica de baja o alta tecnología. La revisión constante del equipo terminal de la víctima será un método *low-tech*, pero la instalación de *key-loggers*, *screen-loggers* o de GPS

[230] En artículo 33 de la Ley 1801 de 2016 hubiere sido el sitio adecuado dentro de la sistematicidad del Código de Policía para consignar la conducta en caso de querer sancionarla policivamente, empero, ninguno de los supuestos de hecho enlistados en la mencionada norma se adecúa a un acecho predatorio o vigilante.
[231] Cfr. *supra*, núm. 8, lit. C., I., cap. II.

que den cuenta de todas las actividades o comunicaciones de la víctima serán métodos *high-tech*, posibilitados por las TIC.

De esta forma, cuando el agente combina tipologías conductuales físicas y tecnológicas estaremos frente a una modalidad de acoso y ciberacoso predatorio. Esta forma de ciberacoso es dependiente del acoso físico, ya que se manifiesta como una *extensión táctica* de aquel para lograr el control que el acechador desea. Aquí, seguimos a YAR con su expresión de *spilled over*; es decir, es una situación en la cual el acoso físico se ha derramado hacía el ciberespacio, o viceversa, el ciberacoso se ha derramado hacía el espacio físico, configurando unas formas de acoso/ciberacoso interdependientes o combinadas que hacen que el acoso/ciberacoso sea mixto y no autónomo o puro.

Cuando existe un ciberacoso mixto, los efectos de la cibercriminalidad en relación con los problemas político-criminales se manifiestan de la misma manera en que lo hacen en los demás delitos cibernéticos amplios o impropios. Esto es, existe una forma de criminalidad que se ha hecho valer de las TIC para ser ejecutada, generando un mayor desvalor, ya que de alguna forma introduce en su modalidad comisiva los problemas propios de la criminalidad cibernética (el anonimato, la accesibilidad, etc.) lo que lo hace merecedor de un mayor reproche. En nuestro medio, entonces, esto se logrará mediante la circunstancia de mayor punibilidad de la parte general o el agravante específico de la parte especial.

Son características propias del acoso o ciberacoso predatorio o de acecho estricto que el agente actúe en solitario sin convocar a terceros y que su objetivo, a su vez, sea individual y no grupal. A diferencia del acoso moral, no se busca la humillación ni el envilecimiento de la víctima, sino su control y el direccionamiento de su voluntad hacia la esfera de poder del autor.

Sobre su relación con la acepción “hostigamiento”, es obvio que la conducta de acecho o de acoso predatorio “hostiga” a la víctima, sea cual sea la tipología conductual ejecutada. Sin embargo, el papel de la palabra “hostigamiento” en este contexto será del resultado de la acción, esto es, será una manifestación de la afectación a la víctima, que ha terminado hostigada por la conducta predatoria. Por el contrario, como adelante se detalla, la palabra “hostigamiento” utilizada en el contexto del acoso moral se usa como sinónimo de una forma estricta de humillación, degradación y envilecimiento de la víctima.

En este orden de ideas, resulta evidente que este tipo de acoso predatorio o de acecho estricto, que se puede ejecutar física o electrónicamente, tornándose en un ciberacoso mixto (superpuesto o derramado) es una conducta disvaliosa y lesiva, en especial en el ámbito de la violencia doméstica o intrafamiliar, lo que hace necesario que sea gestionada por el Estado y objeto de regulación por la

política criminal, en cuanto que esta forma de ha sido una de las herramientas por excelencia de los abusadores para mantener el control sobre sus presas.

2. Acoso sexual

Otra forma de acoso predatorio o de acecho es el acoso sexual. A diferencia de lo señalado por VILLACAMPA ESTIARTE y ALONSO DE ESCAMILLA, tenemos para nosotros que el acoso sexual es una forma de acoso predatorio y no una especie de acoso moral, en cuanto que el agente realiza la búsqueda de cercanía física con la víctima con un propósito sexual, no con el fin de humillar o envilecer. Como todo acoso, el acoso sexual implica un riesgo de afectación psicológica para la víctima y requiere para su estructuración de una serie de actos concatenados que hagan parte de un patrón o curso de conducta sistemático[232].

En el ordenamiento colombiano, este es el único tipo de acoso sancionado penalmente, con pena de prisión de hasta tres años. En su estructura típica, y ello se manifiesta como el hábitat o entorno social que permite este tipo de acoso, se requiere que la conducta se ejecute por el agente con aprovechamiento de una determinada relación asimétrica de poder. En el caso colombiano —pues el asunto varía de ordenamiento en ordenamiento— la cláusula es más amplia, en cuanto que esa relación asimétrica de poder puede manifestarse en las relaciones laborales, educativas, sociales, familiares, económicas, "o cualquier posición manifiesta de superioridad", a diferencia de lo que sucede, por ejemplo, en el ordenamiento español, donde la relación se circunscribe a relaciones laborales, educativas o de salud.

Como se dijo, el hábitat o entorno social que influencia el acto del acoso sexual son las relaciones asimétricas de poder, las cuales no implican un desvalor *per se*. Es decir, la forma jerarquizada en que diversos ámbitos sociales (si no todos) están organizados no es una situación que por sí misma implique valores negativos. Lo desvalorativo que surge de este hábitat o entorno social se manifiesta cuando, en virtud de la relación asimétrica, un sujeto con superioridad sobre la víctima se hace valer precisamente de esa posición ventajosa para hostigar, perseguir, asediar física o verbalmente a la víctima. La influencia de este tipo de relaciones sobre la conducta (*i.e.* la influencia del hábitat o entorno social sobre el punible) es evidente, toda vez que el reproche se erige precisamente por hacerse valer de ese tipo de relaciones para buscar el favor o beneficio sexual. Con ello, queda por fuera del radio del acoso sexual los actos hostigadores o repetitivos, con contenido sexual, en los cuales la relación de poder no exista o el

[232] En este sentido, cfr. Corte Suprema de Justicia, Sala de Casación Penal. Sentencia SP107-2018, rad. 49799, M.P.: Fernando León Bolaños Palacios. También BENAVIDES MORALES, David. "Delitos contra la libertad, integridad y formación sexuales", en CASTRO CUENCA, Carlos G. (coord.). *Manual de derecho penal parte especial*, T. I, 2ª ed., Bogotá, Temis, Universidad del Rosario, 2018, p. 442.

agente no se haga valer de ella. En el estado actual del ordenamiento jurídico colombiano, dichas conductas serán impunes o reconducibles a la injuria por vía de hecho.

El acoso sexual, como el acoso predatorio en sentido estricto, puede *spilled over* al mundo cibernético (o viceversa), cuando los avances intrusivos con contenido sexual se hacen mediante las TIC. Sin embargo, resulta llamativo como el ciberacoso sexual, cuando es entre mayores y a diferencia del *online child grooming*, no busca borrar huellas o esconderse bajo los efectos del anonimato. En este caso, el uso de las TIC se realiza como un refuerzo a la campaña acosadora sexual y, las más de las veces, constituirá prueba de cargo para el acusado de la conducta. Por ello, debe existir un debate que valore la necesidad de considerar a esta conducta como con mayor desvalor o destinataria de mayor reproche. En nuestra opinión, ello podrá ser así, porque a pesar de no tomar ventaja del elemento del anonimato, la conducta sí podrá tomar ventaja de otros elementos característicos de la cibercriminalidad, como la fácil accesibilidad, la automatización al momento de enviar mensajes, la posibilidad de ejecutar la conducta en cualquier tiempo y desde cualquier espacio, lo que generará en la víctima un efecto emocional de desamparo, incluso en su propio domicilio.

De la misma manera que el acoso predatorio o de acecho estricto, el acoso sexual se presenta entre individuos, sin que el agente convoque a terceros a participar del patrón de conducta ni atacando a agrupaciones de personas. Acá, como en el anterior, tampoco hay un curso de conducta que busque la degradación o humillación de la víctima; por el contrario, el patrón conductual, las más de las veces, consistirá en constantes mensajes halagadores con contendido sexual explícito o implícito.

B. Acoso moral

El acoso moral, como se dijo, es un conjunto de actos repetitivos, persistentes e intrusivos que humillan, degradan o envilecen a la víctima, generando un riesgo psicológico para ella, sea mediante la difamación, la amenaza o la intimidación. En estos supuestos, el agente no busca la cercanía física con la víctima; de ahí que este acoso no sea predatorio o de acecho, ya que no hay una persecución que busque controlar a la víctima o mantenerla dentro del ámbito de control, con fines sexuales o no. Contrario a ello, al agente le es irrelevante la cercanía con la víctima, y en el caso de ciberacoso moral estricto (o ciberhostigamiento) es incluso deseable mantener la distancia, con el fin de dificultar la persecución judicial.

Dentro de esta categoría, incluimos el acoso escolar (*bullying* y *cyberbullying*), el acoso laboral (*mobbing*), el acoso inmobiliario (*blockbusting*) y el acoso moral estricto u hostigamiento (*harassment* y *cyberharassment*).

1. Acoso escolar

El acoso escolar también es una forma de violencia y de abuso, de carácter moral. Rechazamos la posición de KIEL, KREMLING y SHARP PARKER que lo ubican como el género de las demás formas de acoso. Por el contrario, tenemos para nosotros que es una especie de acoso psicológico, y a su vez, de acoso moral.

La definición más aceptada de acoso escolar o *bullying* es la del sueco OLWEUS, quien considera que "un alumno es maltratado o victimizado cuando está expuesto repetidamente y a lo largo del tiempo a acciones negativas de otro o de un grupo de estudiantes."[233] De ello, es posible entonces extraer las tres características clásicas del acoso escolar para la doctrina[234]: (i) intención de dañar a una persona; (ii) repetición en el tiempo; y (iii) existencia de un desequilibrio de poder real o imaginado entre el agresor o agresores y la víctima.

En este sentido, resulta evidente su caracterización como acoso moral, en cuanto que busca humillar, envilecer o degradar a la víctima, sea a través de actos de hostigamiento (humillar, difamar, envilecer, degradar) o de intimidación (amenazar). La conducta se puede realizar de forma individual, pero las más de las veces se ejecutará de forma grupal en contra de un solo sujeto.

Así, el hábitat o entorno social que condiciona esta forma de acoso son las relaciones escolares de poder, en las cuales los alumnos buscarán ejercer dominio sobre las víctimas a través de su humillación o degradación frente a sus pares.

Sobre este asunto, existe discusión en la doctrina sobre si el acoso escolar solo puede suceder entre pares (acoso horizontal) o si también pueden participar de él los profesores y miembros del cuerpo educativo; o viceversa, si los alumnos pueden acosar escolarmente a un profesor (acoso vertical). Sobre ello, algunos autores —incluido el padre de estos estudios, OLWEUS— consideran que el matoneo escolar es esencialmente entre pares[235]. Tenemos para nosotros que ello debe ser así, ya que la intervención de mayores tornaría el hábitat que posibilita el acoso escolar —esto es, las relaciones escolares— en uno de relaciones interpersonales, propio del acoso moral estricto u hostigamiento.

---

[233] Citado por GARCÍA GUILABERT, Natalia. *El ciberacoso. Análisis de la victimización de menores en el ciberespacio desde la teoría de las actividades rutinarias*, Buenos Aires, B de F, 2017, p. 22. La Corte Constitucional (Sentencia T-478 de 2015, M.P.: Gloria Stella Ortiz Delgado) también señaló una definición, indicando que acoso escolar o *bullying* es "la agresión repetida y sistemática que ejercen una o varias personas contra alguien que usualmente está en una posición de poder inferior a la de sus agresores."

[234] GARCÍA GUILABERT. *El ciberacoso, cit.,* p. 22.

[235] CASTRO SANTANDER, Alejandro; RETA BRAVO, Cristina. *Bullying blando, Bullying duro y ciberbullying. Nuevas violencias y consumos culturales*, Santa Fe, Homo Sapiens, 2013, p. 52; VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 50.

El acoso escolar, como todo acoso, comporta un riesgo psicológico para la víctima. Precisamente, es en este tipo de acoso donde más se ha manifestado este riesgo, que ha llevado a que víctimas del *bullying* terminen suicidándose antes que seguir soportando el matoneo[236].

Así mismo, como todo acoso, debe ser sistemático, reiterativo, persistente e intrusivo. Con ello, son varias las tipologías conductuales que puede desplegar el acosador escolar o el grupo acosador. En especial, la violación de la información personal de la víctima, la promoción de rumores o falsedades, la comunicación análoga e insistente con la víctima con contenido amenazante o intimidante, e incluso el asalto físico. De esta forma, la conducta también lesiona la libertad y autonomía del estudiante, puesto que lo obliga a tomar decisiones no libremente adoptadas, como cambiar de salón, cambiar de escuela o cerrar cuentas en redes sociales (en el caso del acoso escolar cibernético).

Como otras formas de acoso, las tipologías conductuales pueden "derramarse" hacia el ciberespacio, configurándose un ciberacoso escolar mixto. Así, la táctica sistemática de acoso puede incluir tanto la agresión física y la amenaza directa como los mensajes automatizados repetitivos por Internet, la exclusión de grupos virtuales en redes sociales o grupos de chat, la creación de fotomontajes o *memes* degradantes y de forma prevalente la publicación de información personal de la víctima, en especial a través del *sexting*.

Empero, esta forma de acoso moral comporta una gran similitud con el acoso moral estricto cibernético o el ciberhostigamiento, en cuanto que es posible que el acoso escolar se ejecute enteramente en el ciberespacio, en lo que MIRÓ LLINARES llama como ciberacoso escolar puro[237], en contra posición a una forma mixta que involucrará tácticas de acoso físico como de acoso cibernético, siendo en ese sentido el *cyberbullying* una extensión del *bullying* que busca reforzar el patrón de conducta lesivo.

Este problema social que ha llevado a la muerte a diversos adolescentes atormentados no se manifiesta en nuestro ordenamiento como un delito, por lo que mal podría incluirse su clasificación dentro de alguna forma de criminalidad cibernética. Con todo, si hubiere de considerarse esta conducta como un ilícito o crimen en sentido amplio (tipológico, más no normativo), cabría señalarse que su forma *online* mixta, como también es el acoso predatorio en línea, debe

---

[236] Cfr. CASTRO SANTANDER, RETA BRAVO. *Bullying blando, cit.,* p. 99 y ss.

[237] MIRÓ LLINARES. *El cibercrimen, cit.,* pp. 86-87, sostiene, además, que en esta forma de ciberacoso escolar puro puede no existir relación previa entre el agente y la víctima. Empero, no compartimos tal posición en cuanto que el hábitat social que permite el acoso escolar como forma de acoso moral son las relaciones escolares, en donde puede que, si bien un alumno no conozca *personalmente* a su par, lo cierto es que compartirán espacios comunes dentro de una misma escuela o entre escuelas.

considerarse como un crimen cibernético amplio o impropio, mientras que su forma pura —en donde hay un aprovechamiento al máximo de los problemas político-criminales que el ciberespacio genera— deberá ser considerado como un cibercrimen estricto o propio.

En todo caso, en Colombia este tema, a partir de los hechos citados relacionados con Sergio Urrego (a pesar de que el acoso en su caso no fue ejecutado por sus pares, sino por directivas y profesores de la institución educativa), se tornó en un problema de primera categoría a ser gestionado, por lo que desde la perspectiva administrativa se ordenó a los colegios a adoptar y ajustar sus manuales de convivencia con el fin de gestionar el riesgo de matoneo y las potenciales consecuencias negativas que este tipo de conductas generan. Así, los colegios que fallen en realizar esta gestión podrán ser sancionados administrativamente por las Secretarías de Educación de todo el país.

Lo anterior se comporta en extremo como necesario, ya que los efectos del acoso escolar y en especial del ciberacoso escolar pueden ser nefastos para las relaciones escolares y para el desarrollo vital de los menores. Aquí se vislumbra con claridad como los efectos negativos del ciberespacio pueden incidir en bienes jurídicos personalísimos. Nótese como el ciberespacio transforma las relaciones escolares, en cuanto que traslada a los menores al mundo virtual, el cual se convierte en la isla imaginada por William Golding en su clásico *El Señor de las moscas*: un espacio no regulado por adultos donde los menores sacan a relucir la maldad que en ellos también habita.

2. Acoso laboral

Otra forma de acoso moral que busca la degradación y humillación de la víctima es el acoso laboral o *mobbing*. Esta conducta consiste en el acoso reiterado, sistemático y persistente, en contra de un trabajador producida por sus compañeros de trabajo —*mobbing* horizontal—, sus superiores jerárquicos —*mobbing* vertical descendente— o sus inferiores jerárquicos —*mobbing* vertical ascendente—, que ejecutada durante un lapso temporal genera riesgos psicológicos para la víctima y causa sentimientos de humillación, envilecimiento o degradación[238].

La palabra *mobbing* es una alocución inglesa que viene del verbo *to mob* y que significa acosar, atropellar o atacar en masa a alguien. De ahí que se considere que el *mobbing* comporta un patrón de conducta grupal en contra de un individuo. Empero, la *praxis* ha demostrado que un solo sujeto —en especial cuando es el superior jerárquico del empleado— puede desplegar un patrón de conducta

[238] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 48, además, señala que un sector de la doctrina incluye como finalidad del acoso laboral la expulsión o autoexclusión del empleado del lugar de trabajo.

acosador en el ámbito laboral y lograr los objetivos de degradación o autoexclusión del empleado. De esta forma, la conducta es lesiva de la libertad y autonomía del trabajador, al direccionar su voluntad hacía una decisión que no adopta libremente.

El hábitat o entorno social en el cual se desarrollan estas conductas sistemáticas de acoso son las relaciones laborales o del trabajo, las cuales se deben ver gobernadas por el respeto, la equidad y la paridad.

Existen diversas tipologías conductuales del acoso laboral, como el maltrato laboral (actos de violencia física o moral), persecución laboral (actos arbitrarios que buscan inducir la renuncia del trabajador), la discriminación laboral (el tratamiento diferenciado de trabajadores sin justificación), entorpecimiento laboral (acciones tendientes a entorpecer el trabajo de la víctima), inequidad laboral (asignación de funciones a menosprecio del trabajador) y la desprotección laboral (conductas tendientes a poner en riesgo la integridad del trabajador).

Estas tipologías podrán ejecutarse a través del ciberespacio, empero, carecen de la suficiente incidencia (o pureza, siguiendo la terminología expresada en este trabajo) para considerar dichas conductas como autónomas en una relación acoso laboral/ciberacoso laboral. Así, de forma diáfana, se ve que el apoyo en las TIC es una mera instrumentalización para llevar a cabo la táctica acosadora, sin que existan mayores efectos del ciberespacio sobre la forma en que la problemática se manifiesta.

Además del riesgo psicológico, la conducta lesiona la libertad y autonomía de la víctima, en especial cuando se logra, como lo señaló VILLACAMPA ESTIARTE, la renuncia o la autoexclusión del trabajador del ámbito laboral.

Estas conductas no son delitos. Ellas se consideran infracciones administrativas, sancionables por el Ministerio del Trabajo.

En Colombia, la problemática fue atendida mediante la Ley 1010 de 2006. Empero, como se citó en la introducción del trabajo, son pocas las decisiones que se han tomado a favor de los denunciantes.

3. Acoso inmobiliario

Una forma de acoso poco conocida en Colombia es el *blockbusting* o acoso inmobiliario. La conducta consiste en desplegar un patrón de conducta hostigador con miras a expulsar de una vivienda a un arrendatario, ya sea por medio de tácticas de humillación o envilecimiento, ya sea por medio de tácticas más directas y físicas, como omitir reparaciones necesarias, cortar el suministro de servicios

públicos, emprender supuestas obras locativas de mejoras para aburrir al inquilino, introducir al edificio a vecinos indeseables, etc.[239]

La conducta puede tener efectos psicológicos sobre la víctima, en cuanto que puede verse inmerso en una situación de desamparo y sin vivienda digna; pero, además, también lesiona la libertad y autonomía del sujeto, habida cuenta que la acción acosadora direcciona su voluntad a abandonar la vivienda.

El hábitat o entorno social en el que se desarrollan estas conductas es en las relaciones contractuales especiales entre arrendador y arrendatario.

La conducta, como la anterior, no sostiene una forma de acoso cibernético autónomo que implique problemas jurídicos propios del uso del ciberespacio. A lo sumo, el uso de las TIC tendrá como propósito la comunicación insistente que busque la salida del inquilino de la vivienda.

Esta forma de acoso moral no es sancionada de forma especial en Colombia, como sí en Estados Unidos o en España. Sin embargo, puede generar consecuencias jurídicas a nivel contractual, que supongan pagos de indemnización de perjuicios por incumplimientos contractuales de mala fe a la luz de la normatividad especial civil y comercial.

4. Acoso moral estricto (hostigamiento) y ciberacoso moral estricto (ciberhostigamiento)

El acoso moral estricto, que llamamos también *hostigamiento*, es una forma especial de acoso moral que puede suceder en el mundo físico, pero cuyo mayor desvalor y cuya mayor necesidad de gestión jurídica se da en el ciberespacio, es decir, respecto del ciberacoso moral estricto o ciberhostigamiento.

La conducta consiste en el despliegue de un conjunto de actos reiterativos, persistentes, intrusivos y concatenados que conforman un curso o patrón de conducta que tiene por fin el envilecimiento, la humillación, la degradación o la intimidación de la víctima. Este tipo de conducta no es ajena al mundo físico, en cuanto que es posible realizar este tipo de actos de forma reiterativa mediante formas de comunicación análogas (cartas, teléfono, personalmente). Sin embargo, no debe caber duda de que es a partir de la introducción de las nuevas TIC y la evolución del Internet a la Web 2.0 que estas conductas adoptaron nuevos niveles de lesividad y peligrosidad, precisamente por todas las posibilidades que el ciberespacio otorga para su ejecución. Es decir, si bien son conductas “clásicas” o “preexistentes” a las nuevas TIC, es a partir de ellas que su gestión preventiva les otorga gran relevancia penal.

---

[239] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 52.

De esta forma, el ataque tiene una gran potencialidad de lesionar al bien jurídico libertad y autonomía (cibernética) ya que por temor u hostigamiento la víctima decide suprimir su identidad virtual, dejando de frecuentar grupos de chats, cerrando cuentas en redes sociales y sintiéndose en un estado de indefensión psicológica, incluso en su misma vivienda, ya que el ciberespacio, al contraer el espacio-tiempo, dará a entender a la víctima que ningún lugar es seguro.

Desde esta óptica, es posible desde ya desligar este tipo de acoso moral del acoso predatorio, ya que no se identifican en su hábitat social ni en la naturaleza de la conducta.

Mientras que el acoso predatorio es un acecho físico o virtual, el acoso de hostigamiento es una degradación física o virtual. Este punto es relevante en el entendimiento del fenómeno general del acoso, ya que la gran discusión científica acerca de la autonomía o no del acoso físico en relación con el ciberacoso se ha centrado en identificar al *stalking* de acecho en relación con el *cyberstalking* moral, que nosotros denominados *cyberharassment* o ciberhostigamiento. Así, desligar esa identificación es lo que nos permite conceptualizar debidamente los diferentes ámbitos y formas de acoso.

Por ello, tenemos para nosotros que el ciberhostigamiento *no debe ligarse* al acoso de acecho, ya que son conductas diferentes y diferenciables. Así, nos fue posible concluir que el ciberacoso de acecho, en efecto, es una *extensión* (mixta o derramada) del acoso de acecho; mientras que el ciberhostigamiento —ciberacoso moral estricto— es una forma autónoma y diferente del acoso/ciberacoso de acecho, e incluso, del acoso moral estricto físico (que podrá considerarse contravención policiva y no delito), ya que las posibilidades que el ciberespacio le otorga a esta cibercriminalidad social concreta supera con creces lo que podría realizarse en el ámbito de su modalidad física o análoga.

Contrarios a nuestra posición de autonomía del ciberhostigamiento son, por ejemplo, CLOUGH, PITTARO y NAVARRO[240]. También SHERIDAN y GRANT[241], quienes señalan que no hay autonomía en cuanto que el proceso de acoso es igual, el efecto sobre las víctimas y terceros es igual, la respuesta de las víctimas es igual y el género sexual del acosador es igual. Sin embargo, otra parte de la doctrina sí reconoce dicha autonomía, si bien no a partir de la misma fundamentación aquí desarrollada —cuyos pilares son la existencia de una cibercriminalidad social a partir de la Web 2.0 y la diferencia de hábitats o entornos sociales que alejan cada una de las formas de acoso y ciberacoso existentes—.

[240] Cfr. *supra*, nn. 114, 118 y 134 respectivamente.

[241] SHERIDAN, Lorraine; GRANT, Tim. "Is cyberstalking different?", en *Psychology Crime and Law*, No. 13 (6), Milton Park, Taylor & Francis, 2007, pp. 3 y ss. Accesible en: [https://www.researchgate.net/publication/40500406_Is_cyberstalking_different]

En este sentido, BOCIJ y McFARLANE[242] señalan que son diferentes ya que (i) los gobiernos y la *mass media* así lo entienden; (ii) el acosador no se comporta igual que el ciberacosador; (iii) y cada nueva tecnología genera nuevos crímenes.

Para entender mejor los contornos de la figura en comento, habrá que ahondarse en las ideas ya esbozadas acerca del profundo cambio generado por la Web 2.0 en las formas de relacionamiento social. Es decir, el surgimiento de un hábitat o entorno social capaz de moldear la forma en cómo se desenvuelve la vida física y la vida cibernética, al punto de generar relaciones sociales cibernéticas o relaciones criminales cibernéticas (o lo mismo: una nueva cibercriminalidad social —estricta o propia—). Con ello se evidenciará que, contrario a lo señalado por SHERIDAN y GRANT, el proceso de ciberacoso no siempre es igual al del acoso; la respuesta de las víctimas a los ataques ciberacosadores no son siempre iguales respecto de su respuesta a los ataques acosadores; y el género sexual del ciberacosador no es siempre el mismo que el de los acosadores.

Como ya arriba se dijo, puede que las conductas desviadas que hacen parte de la cibercriminalidad social que la Web 2.0 ha permitido sean conductas ya viejas, ahora canalizadas a través de las TIC y el ciberespacio. Ello no obsta para considerar a estos delitos como verdaderos cibercrímenes sociales o personales en sentido estricto, ya que la forma en que ahora se manifestarán implican elementos especiales que nacen a partir de la nueva oportunidad delictiva que ciberespacio provee. Así, el Internet y el ciberespacio funcionaron como catalizador de la evolución de conductas tradicionales que hoy son diferentes y requieren de atención focalizada, porque no es lo mismo, por ejemplo, exponer un discurso de odio en la plaza pública que en la plaza cibernética. Estos dos injustos difieren en tal medida que la segunda conducta genera un daño inmensamente mayor que la primera. Ello mismo puede predicarse del acoso moral estricto u hostigamiento en relación con el ciberacoso moral estricto o ciberhostigamiento.

Si bien es cierto que en un principio el Internet se usó para la gestión de información y lograr un mayor acceso a ella, y que en sus labores las prácticas predominantes eran las transacciones económicas; hoy ello ya no es así: además de lo anterior, el ciberespacio es un lugar en el cual las personas contactan con otras, crean redes de amigos o profesionales y en general lo usan para *relacionarse* como seres sociales que somos. Si esto es así, es posible afirmar que los sujetos desarrollan su personalidad (digital) en el ciberespacio, exponiendo en dichas interacciones sociales su forma vital y su forma de ser, de donde se pueden extraer bienes jurídicos que orbitan en el ciberespacio para ser

[242] BOCIJ, Paul; McFARLANE, Leroy. "Seven fallacies about cyberstalking", en *Prison Service Journal*, No. 149, Gloucestershire, Center for Crime and Justice Studies, 2003, pp. 37 y ss. Accesible en: [http://www.paulbocij.net/index.php/downloads]

valorados a partir de relaciones sociales positivas, o para ser degradados y lesionados a partir de relaciones sociales negativas de carácter criminal.

Podría indicarse en contra de esta posición que hace énfasis en el profundo cambio de la Web 2.0 sobre las relaciones sociales, que desde el principio del Internet y del ciberespacio existían relaciones sociales de algún tipo, puesto que con el surgimiento del Internet vino adjunto el correo electrónico —medio de comunicación social— y las páginas web, navegables desde los albores del ciberespacio mediante *browsers*, como Netscape.

Sin embargo, se insiste, ello era antes de la Web 2.0. En aquellos años era muy poco el tráfico comunicativo a través de correos electrónicos o de páginas web que no tuvieran una función laboral, económica o informativa. En cambio, desde mediados de la década de los 2000, surgieron formas sociales de comunicación que ya se vincularon con el desarrollo de la personalidad de los ciudadanos digitales —en especial de los nativos digitales—, a través de las redes sociales como MySpace o Facebook[243], o incluso otras localizadas geográficamente, como Orkut en Brasil, o Hi5 en Estados Unidos.

Lo anterior llegaría a dimensiones inimaginables con el desarrollo de los *smartphones*, proceso en el cual llevó la batuta Research In Motion (RIM) con el BlackBerry, y que Apple innovó hasta la cuasi perfección con el iPhone. Con ello, la conexión al ciberespacio ya no fue un asunto de esperar a que terminara la jornada escolar o laboral para conectarse desde el PC de la vivienda, sino que esa conexión era *sin solución de continuidad*, casi perpetua.

Con todo ello, se le permitió al usuario la gestión de su propia identidad digital y de su personalidad de forma permanente en línea, y así posibilitó nuevas formas de interacción y concreción de relaciones sociales. Este tipo de vinculación interpersonal y social se manifiesta con igual importancia a que si el sujeto estuviera haciendo amigos en una reunión social física, e incluso, podría llevar a otras dimensiones de interrelación, ya que el ciberespacio derrota cualquier barrera espacio-temporal, tal vez siendo la única interacción que se le escapa a ese reino digital el contacto físico-sexual, lo que, hay que decirlo, ya también se ha ido derribando mediante el sexo virtual a distancia (piénsese en el lucrativo negocio de las *webcam*); o incluso, en el futuro próximo con la realidad virtual.

Todo esto generó una oportunidad inaudita para el crimen. Al desarrollar la identidad mediante la comunicación de los aspectos personales de la vida, se

[243] MIRÓ LLINARES. *El cibercrimen, cit.,* p. 123, señala que el éxito de las redes sociales estuvo en que pudo integrar en un solo medio todo lo que antes estaba disperso: mensajería instantánea, grupos de chat, creación de webs, diarios electrónicos, blogs, correo electrónico, álbumes de fotos, selección de música y video, etc.

generó el espacio perfecto para poder aprovechar esa gestión de identidad para la comisión de conductas disvaliosas. El ciberespacio, entonces, generó una oportunidad cuantitativa —más crímenes— y cualitativa —mayor daño— para ejecutar conductas desviadas lesivas.

En concreto, el ciberespacio le dio oportunidad al ciberacoso de ser ejecutado virtualmente en contra de cualquier persona. A diferencia de los otros tipos de acoso moral e incluso de acoso predatorio, el ciberhostigamiento puede dirigirse en contra de cualquier extraño o persona con la cual el agente no haya tenido ningún tipo de relación previa. Esto implica que todo usuario de la web es una *potencial* víctima de un ciberacosador moral dispuesto a degradarlo hasta el punto de suprimir su voluntad cibernética.

En este mismo sentido, si es posible que el ciberhostigador se dirija en contra de cualquier usuario, entonces también podrá agruparlos para atacarlos. El caso más mediático de los últimos años es el de “La Ballena Azul” y “Momo”. Estas actividades, que macabramente fueron bautizadas como “juegos” por los agentes o agente detrás de esas campañas de ciberhostigamiento, consistían en direccionar la voluntad de los menores —grupo especialmente vulnerable en el ciberespacio— hasta someterlos a realizar actos lesivos para ellos mismos. El *modus operandi* consistía en comunicarse con los menores a través de mensajes automatizados, solicitando la realización de determinados retos. Cuando las víctimas fallaban en lograr el reto —ya sea por no querer ejecutarlo o por genuinamente no haber tenido la capacidad de hacerlo—, emprendían la campaña de acoso cibernético moral comunicando mensajes amenazantes y degradantes, del tipo “sabemos lo que haces”, “eres una basura por no hacer el reto”, “le diremos a los demás en el colegio”, *et alters*. Al final, muchas víctimas cambiaban de números de celular o de cuentas digitales, sin llegar a lograr escapar del patrón de conducta, por cuanto que, por medio de algoritmos, los agentes continuaban la comunicación hostigadora en las nuevas cuentas digitales de las víctimas. En el peor de los casos, el ciberacoso moral llevaba a las víctimas a ejecutar los retos autolesivos o a autolesionarse con tal de escapar la campaña de degradación, intimidación y humillación.

Los menores también se han visto expuestos a situaciones de acoso moral estricto a través de las consolas de videojuegos —los casos más recientes en relación con el exitoso juego *online Fortnite*—, ámbitos virtuales en los cuales comparten espacio con adultos, quienes también emprenden campañas de desprestigio y humillación que tienen repercusiones para ellos, en cuanto que son degradados en frente de sus pares video jugadores.

El anonimato proporcionado por la Red también aumenta el desvalor de estas conductas, ya que trasmite una sensación de desamparo y de desasosiego para la

víctima el hecho de no conocer a su atacante —puede ser un compañero o un desconocido, puede estar cerca o puede estar lejos—. A su vez, dicha característica hará más difícil la persecución y judicialización, con lo que se hace necesario el desarrollo de técnicas forenses que permitan rastrear a los atacantes, lo que en el mundo del Internet genera escozor, ya que dicha situación demerita la neutralidad y libertad de la Red.

Otro de los efectos más significativos del ciberespacio en la configuración de la cibercriminalidad social —con efectos directos en la conducta de ciberhostigamiento— es la ruptura que se genera sobre los entendimientos clásicos de espacio y de tiempo.

En relación con el espacio, la diferencia entre el espacio físico y el espacio cibernético, que a su vez permite fundamentar la diferencia entre la criminalidad social física y la criminalidad social cibernética, se hace evidente a partir del hecho que permite la existencia de uno u otro. Es decir, el ciberespacio solo existe en cuanto espacio relacional intersubjetivo. La "realidad" de dicho reino virtual solo existe en cuanto intercambio de acción comunicativa. Una "red" sin interacción de los sujetos que la componen no es una red. El ciberespacio, entonces, existe en cuanto existen interacciones en su red comunicativa. Ello ya delinea una primera gran diferencia con el espacio físico, el cual no depende de la interacción de sus miembros. Incluso sin interacción, el espacio físico existirá. La interacción de dos sujetos en una esquina será interacción social, y al finalizar dicha interacción, la esquina seguirá existiendo. Por el contrario, al no existir interacción en el ciberespacio, él agotará su existencia. De esta forma, ahí donde el espacio físico otorga protección (el domicilio, por ejemplo), el espacio cibernético no lo otorgará, ya que éste existe *dentro* del domicilio, porque ahí es donde la interacción social-virtual se está desarrollando.

Además, más allá, una segunda gran diferencia entre el espacio físico y el espacio cibernético es la eliminación de medición de distancias en el ciberespacio. En este lugar cibernético *no existen* las distancias, como sí existen y sí condicionan al sujeto en el espacio físico. YAR señala que en el ciberespacio todas las distancias son iguales[244]. No se está más lejos ni se está más cerca: solo se está. Esta contracción espacial implica una potencialización de la interacción comunicativa. Si antes solo era posible comunicarse con el vecino; y después con la comunidad cercana; y después con los que ostentaran un teléfono; hoy es posible comunicarse con cualquier que tenga acceso a la Red. La contracción espacial volvió al globo en una aldea, haciendo posible la idea de la "aldea global", como lo pensó el sociólogo canadiense Marshall McLuhan.

[244] YAR, Majid. "The novelty of cybercrime: An assessment in light of routine activity theory", en *European Journal of Criminology*, No. 4 (2), Thousand Oaks, SAGE, European Society of Criminology, 2005, p. 408.

Lo anterior tiene efectos sobre el ciberhostigamiento, ya que permite desplegar conductas de interacción comunicativa lesivas respecto de cualquier sujeto en cualquier parte del mundo. Al ser un "espacio-no espacio" —un espacio deslocalizado que al mismo tiempo es y no es (como el *Aleph* borgiano)— las dificultades jurisdiccionales que se suscitan son grandísimas, en cuanto que genera conflictos de competencia, problemas de impunidad y dificultará la colaboración, nada de lo que se manifiesta en el acoso moral físico y localizado. En el ciberhostigamiento, la persecución judicial se hará muchísimo más difícil y parece ser que los instrumentos vigentes y actuales de cooperación internacional, como la extradición, son insuficientes. Tal vez la única vía para poder gestionar esta problemática frente a este tipo de cibercriminalidad social sea por medio de la integración normativa de instrumentos internacionales[245], es decir, mediante la creación de un verdadero supra ordenamiento jurídico.

Así mismo, el tiempo también muta su naturaleza en el ciberespacio. El ambiente cibernético trasmite una característica de *atemporalidad*, en cuanto que lo que ahí sucede puede fijarse infinitamente, ya sea por su rapidísima reproducción o por la imposibilidad de determinar las fuentes de multiplicación. Lo anterior transforma la potencialidad del daño a una capacidad inimaginable, habida cuenta que, por ejemplo, conductas de ciberhostigamiento podrán fijarse de forma perenne en el tiempo. Así, hasta que ocurran las vaticinadas catástrofes del fin de mundo, el ciberespacio será sempiterno, convirtiendo en inmortal lo que antes tenía expiración en el mundo físico. En este sentido, la difamación, la publicación de imágenes intervenidas y editadas degradantes o la publicación de información sexual e íntima de la víctima como formas de hostigamiento moral mediante las TIC, podrán fijarse y reproducirse de tal manera en el ciberespacio que el daño que estas conductas de acoso moral generen sea altamente lesivo. Al momento de redactar estas líneas, habían transcurrido solo unas semanas desde que el mundo fue testigo del suicidio de Verónica[246], una madre de dos hijos, que con 32 años decidió terminar su vida al haberse publicado un video íntimo suyo, el cual circuló en redes por su ámbito laboral y social. Nada pudo hacer para evitar que el video se reprodujera de forma viral e interminable por medio de la Red.

Ahora, dicha conducta genera una discusión conceptual relevante, toda vez que en este supuesto de hecho podría argumentarse que no se ejecutó una conducta de acoso, ya que no se desplego una campaña o patrón de conducta. Por el contrario, el agente solo realizó la conducta una sola vez. Nuestra posición sobre

---

[245] Cfr. más sobre esta necesidad en RIQUERT, Marcelo A. "Repensando cómo funcional la ley penal en el ciberespacio", en RIQUERT, Marcelo A (coord.). *Ciberdelitos,* 2ª ed., Buenos Aires, Hammurabi, 2019, pp. 26 y ss.

[246] [https://www.lasexta.com/noticias/sociedad/madre-suicida-madrid-difundirse-antiguo-video-sexual-suyo-trabajo_201905285ced13fb0cf21b72629c0631.html]

este asunto es considerar que el desvalor no deviene de que el agente *directamente* realice varios actos repetitivos de acoso/ciberacoso, sino que *existan* varios actos repetitivos de acoso/ciberacoso, ya sea realizados directamente por el agente, o ya sea valiéndose de terceros (autoría mediata que abarcaría tanto al acoso físico como al ciberacoso) o mediante la automatización que el ciberespacio y la informática permiten (para el caso del ciberacoso).

Así las cosas, si bien es cierto que el agente solo realizó una acción, y no un conjunto de actos concatenados que forman un curso de conducta, en ese punto se debe diferenciar entre la acción aislada que genera la lesión y la acción individual que pone en marcha la campaña acosadora. En el primer caso, la conducta debe reconducirse hacia otro tipo penal, como la injuria. Esto habida cuenta que una sola acción fue la que lesionó la integridad moral de la víctima. Empero, en el segundo caso, el acoso sí podrá constituirse, ya que es posible que el ciberacosador realice una sola acción con miras a que terceros, sea de forma consciente o inconsciente (en lo que se estructurará una autoría accesoria o autoría mediata), emprendan la campaña acosadora. Éste último caso sería aquel (fallado en Estados Unidos[247]) en el que el autor publica información y fotomontajes de la víctima en un sitio web de prostitución para que terceros hostiguen a la víctima solicitándole servicios sexuales que en realidad no presta.

En este orden de ideas, hay que admitir y diferenciar las situaciones en las cuales el agente realiza una sola acción lesiva de la integridad moral o realiza una sola acción lesiva de la integridad moral que tiene como efecto que terceros emprendan la campaña de ciberacoso, logrando así también la lesión de la libertad y autonomía de la víctima al ser sometida a un curso de conducta, ejecutado por terceros, pero propiciado por el autor.

Con base en todo ello, es posible sustentar la autonomía lesiva del ciberacoso moral estricto o del ciberhostigamiento como conducta necesitada de punición, ya que los efectos que el ciberespacio le otorga a esta conducta son diferenciables y desastrosos. Este hábitat o entorno social —la incidencia de la Web 2.0 en la configuración de una verdadera cibercriminalidad social— determina los contornos del injusto criminal que el ciberhostigamiento comporta.

En relación con las tipologías conductuales, como ha sido una constante en la explicación de este trabajo respecto de todas las formas de acoso, podrá ser combinada entre ellas o insistente sobre una de ellas.

•

Así se resume la clasificación realizada:

[247] Cfr. PITTARO. “Cyberstalking”, *cit.,* pp. 282-283.

III. Sobre el bien jurídico tutelado

La manera en que se ha realizado la conceptualización del acoso, del ciberacoso y de sus diversas tipologías de acecho o moral, ponen de presente la naturaleza pluriofensiva de dichas conductas. En lo concerniente al acoso moral estricto (hostigamiento) y el acoso moral estricto cibernético (ciberhostigamiento) ello se hace más evidente, en cuanto que la amalgama de tipologías conductuales que allí caben son tan variadas que así mismo se manifiesta la variedad de intereses jurídicos valiosos dignos de protección: la intimidad, el buen nombre, la integridad moral, la salud psicológica, la libertad de acción, la libertad de autodeterminación, la seguridad personal, la seguridad cibernética, etcétera.

La doctrina[248] ha discutido acerca de cuál es el bien jurídico tutelado por las conductas acosadoras. De allí han surgido dos posiciones contrapuestas: de un lado, el bloque que esgrime la prevalencia del bien jurídico de la integridad moral, y de otro, el bloque que da preeminencia al bien jurídico libertad y autodeterminación.

---

[248] Con referencias, cfr. LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso, cit.,* pp. 21-23.

La integridad moral ha sido entendida en nuestro medio como una contraparte de la integridad física o corporal, compuesta "por un conjunto de bienes integrado principalmente por el honor, la honra y el decoro, pero que en todo caso se fortalece con el concepto de dignidad humana"[249].

Partiendo de ese entendimiento, no adoptamos la posición que pone en primer plano de protección a la integridad moral, teniendo en cuenta que no todas las tipologías de acoso psicológico delineadas tienen como fin el envilecimiento, la humillación o la degradación (propias solo del acoso moral), que serían modalidades conductuales que lesionarían el sentimiento de honor u honra de una persona. Piénsese en el acoso predatorio estricto o el acoso sexual, situaciones en las que no existe envilecimiento o humillación, sino por el contrario, adulación y exaltación.

Más aún, debe considerarse que en el acoso moral y su modalidad cibernética el envilecimiento, la degradación y la humillación son formas de ejecución de la conducta y no solamente la motivación o el fin de la misma. En el caso del acoso moral cibernético, por ejemplo, es posible que la táctica del ciberacosador sea la de envilecer o humillar a la víctima, pero más allá de eso, su motivación sea la de la exclusión o autoexclusión del ciberespacio, resultando lesionada la integridad moral, pero también el bien jurídico de la libertad y la autodeterminación.

Por otro lado, la libertad y la autonomía, a pesar de que no ha sido históricamente pacífica su conceptualización filosófica ni su ejercicio práctico y material, deben tenerse como elementos fundamentales de los modernos Estados constitucionales. En efecto, la libertad del ser humano ha sido valorada de forma positiva en cuanto que ella se entiende "como una garantía irrenunciable de la vida moderna en la que el ser humano debe coexistir en sociedad para poder lograr sus fines esenciales y satisfacer sus necesidades básicas."[250] No podría el ciudadano ser y desarrollarse en sociedad si no existe garantía de su libertad para decidir, ejecutar y en general, para obrar.

Es por ello que la necesidad de protección de este bien jurídico deviene de la Constitución misma, en donde se ha consagrado como derecho fundamental el libre desarrollo de la personalidad y la autonomía del sujeto para, en términos de dignidad, vivir como quiere y de acuerdo con su plan de vida.

Así, en punto de las conductas acosadoras, puede afirmarse que la lesión prevalente sobre la víctima consiste en la deformación de su autonomía, tanto en

---

[249] CÓRDIBA ANGULO, Miguel. "Delitos contra la integridad moral", en *Lecciones de derecho penal parte especial*, V. I, Bogotá, Universidad Externado de Colombia, 2019, p. 325.

[250] SAMPEDRO ARRUBLA, Camilo. "Delitos contra la libertad individual y otras garantías", en *Lecciones de derecho penal parte especial*, V. II, Bogotá, Universidad Externado de Colombia, 2019, p. 326.

fase de configuración de la decisión libre como en la fase de ejecución de esa decisión. Nótese como tantos las conductas de acecho predatorias como las conductas de acoso moral afectan la autodeterminación de la víctima y la ejecución de decisiones libres que se hubieren tomado y realizado si la interferencia delictiva del acoso no existiera en la ecuación.

Ejemplo de lo anterior es cuando una víctima de un acoso de acecho decide no salir de su domicilio, cambiar de vivienda o de celular por temor a seguir recibiendo contactos no deseados del *stalker*. Lo mismo sucede con la víctima del acoso moral, que para evitar la campaña de humillación o envilecimiento decide cerrar sus cuentas en redes sociales, cambiar de usuario de chat o dejar de frecuentar los sitios de socialización cibernéticos, en los que desarrollaba y proyectaba su personalidad, por temor a seguir recibiendo amenazas o tratos degradantes que lo demeriten en el nivel subjetivo y también en el nivel objetivo frente a los pares cibernéticos.

En este sentido, defendemos la posición que señala que la conducta de acoso, en medios físicos o cibernéticos, tiene por fin doblegar la voluntad de la víctima y la libertad de su autodeterminación, encauzando la toma y ejecución de decisiones que deberían ser libres en función del riesgo psicológico que el acoso genera en la víctima. Es decir, en vez de tomar decisiones libres en función del libre desarrollo o de la dignidad buscada por el sujeto pasivo, éste deberá introducir dentro de la ecuación de la toma de decisiones, el riesgo que los contactos acosadores le generan o pueden generarle.

En este orden de ideas, un argumento importante a favor de esta posición, es que mientras que solo algunas formas de acoso lesionan la integridad moral, todas ellas lesionan la libertad y la autodeterminación.

Por estas razones, adoptamos la posición que le da preeminencia a la protección de la libertad y a la autodeterminación, sin dejar de afirmar que otros bienes jurídicos también se ven afectados por estas conductas, en especial, la salud psicológica (común a todas las formas de acoso), la seguridad personal (también común a todas las formas de acoso), la libertad sexual (propia del acoso predatorio) o la integridad moral (propia del acoso moral).

Ahora, sin entrar a discutir los modernos debates acerca de la legitimidad de la teoría del bien jurídico para fundamentar la procedencia de la intervención penal, lo que sería un asunto que excedería la conceptualización pre jurídica que en este trabajo se quiere realizar, es importante señalar como esta interpretación del bien jurídico protegido cumple con los principios orientadores de la necesidad de protección jurídico penal.

Así, sostenemos que nuestro entendimiento conceptual del acoso psicológico, en especial del acoso moral estricto y su vertiente autónoma cibernética, cumplen con el principio de lesividad, principio de fragmentariedad, principio de prevalencia del interés público en la criminalización y el principio de correspondencia de la criminalización con la realidad social.

En relación con el principio de lesividad, los estudios de prevalencia dan cuenta de la aptitud de estas conductas para afectar la convivencia social externa, en especial, la convivencia pacífica de las libertades contrapuestas. En este sentido, existe una dañosidad social de la conducta que afecta múltiples intereses personales (ya descritos), que son necesarios para el correcto funcionamiento social e individual.

Así mismo, se cumple con el principio de fragmentariedad, en cuanto que la gravedad de estas conductas, que pueden llevar al suicidio, la depresión o la autoexclusión, merecen de una reacción igual de grave, administrada por el sistema penal. Esto es, dado el carácter fragmentario del derecho penal, que implica que solo deba poner atención a las situaciones más graves que se susciten en sociedad, surge como necesario determinar si cada situación conflictiva reviste la gravedad necesaria. Como se ha propuesto y evidenciado a lo largo de este trabajo, los riesgos psicológicos y personales que se ciernen sobre las víctimas del acoso, en medios físicos o cibernéticos, es de tal magnitud que se ha hecho necesaria su legislación y la implementación de políticas públicas de autoprotección. Por ello, nos es posible afirmar que este fragmento de conflicto social requiere de la especial atención del derecho penal.

El principio del interés público también se encuentra realizado, considerando que los conflictos que se generan por la desviación acosadora pueden ser generalizados y afectar a todas las gamas de la sociedad, afectando el funcionamiento social en su conjunto.

Finalmente, también existe cumplimiento del principio de correspondencia con la realidad social, ya que los estudios empíricos, en especial los sectorizados por poblaciones vulnerables, han dado cuenta de que el problema existe en América Latina, generando daños sociales que pueden ser irreversibles y cuyo desvalor conductual no ha sido debidamente atendido por los ordenamientos jurídicos, incluyendo el colombiano.

IV. Delimitación del ciberacoso moral estricto con otras conductas del ordenamiento jurídico

Otra aproximación a la conceptualización del ciberacoso moral estricto estará dada por la exclusión, desde una perspectiva dogmática, de esa conducta de otras

acciones lesivas de la autonomía o de la libertad, como son los delitos de constreñimiento ilegal (coacciones en el derecho comparado) y de amenazas, o lesivas de la integridad moral, como la injuria y la calumnia.

En términos criminológicos y jurídicos, no es posible adecuar las conductas acosadoras o ciberacosadoras con las conductas de coacciones o de amenazas ya que el acoso y el ciberacoso tipológicamente sobrepasan los límites de sanción de esas conductas. En efecto, una conducta acosadora o ciberacosadora puede ser coactiva o puede ser amenazante —de hecho, algunos ordenamientos jurídicos reclaman la expresión amenazante para poder sancionar el acoso, como Canadá y algunos estados de los Estados Unidos—, pero también puede no ser ninguna de ellas dos.

En relación con el acoso, piénsese en la búsqueda de cercanía física. Este tipo de conducta no es *per se* coactiva, en cuanto que no se ejerce violencia física ni moral; incluso, la víctima puede no conocer que la acechan (y aun así consumar la conducta, de acuerdo con los ordenamientos que solo exigen el resultado jurídico de peligro).

En relación con el ciberacoso, piénsese en la difusión de información personal de la víctima. Con ello, no hay una violencia física o moral explicita que doblegue la libertad de la víctima. Si el delito de constreñimiento ilegal implica ejercer violencia física o moral *sobre* la víctima para doblegar su voluntad a tolerar, hacer u omitir[251], mal podría adecuarse ello a la divulgación de imágenes íntimas si en ese supuesto ni siquiera hay un acto comunicativo entre victimario y víctima, sino entre victimario y público.

Además, en el derecho comparado, en especial en el ordenamiento español, la adecuación de supuestos de acoso o ciberacoso al delito de coacciones conlleva dos críticas más. La primera, que en ese ordenamiento se ha rechazado la espiritualización y volitización del concepto de violencia, para incluir en él, además de la violencia física, la *vis compulsiva*[252]*,* que sería la única forma de acercar al acoso y ciberacoso a la coacción, a falta de violencia física en esas conductas. La segunda, en relación con el objeto de protección, se señala que en el acoso y ciberacoso se protege desde el inicio de la formación de la voluntad, mientras que en las coacciones se lesionada la voluntad ya formada[253].

---

[251] GARZÓN ROA, Andrés. "Delitos contra la libertad individual y otras garantías", en CASTRO CUENCA, Carlos (coord.). *Manual de derecho penal parte especial*, T. I, 2ª ed., Bogotá, Temis, Universidad del Rosario, 2018, p. 310.

[252] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 238; LORA MÁRQUEZ. *Estudio jurídico doctrinal del delito de acoso, cit.,* p. 13; LORENZO BARCENILLA. *Stalking, cit.,* p. 19.

[253] VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 237; LORENZO BARCENILLA. *Stalking, cit.,* p. 18.

Empero, lo más relevante en diferenciar estas conductas es que mientras que el constreñimiento ilegal o coacciones no requiere de la campaña sistemática, el acoso y ciberacoso sí. De esta forma, es posible que un hecho aislado con suficiente entidad lesiva sea un constreñimiento ilegal, pero él habrá de trasladarse al acoso/ciberacoso si se compone de un patrón de conducta, sin perjuicio de que además ello sea así por el carácter subsidiario que ese tipo penal tiene en nuestro ordenamiento.

Frente al tipo de amenazas, se pueden realizar las mismas consideraciones respecto de que no todo patrón de conducta es amenazante o intimidante, pues puede ser solo degradante —en el caso del acoso moral— o solo intrusivo —en el caso de acoso de acecho—. Es decir, pueden desplegarse actos concatenados disvaliosos sin siquiera hacer alguna alusión a algún mal que se vaya a causar a la víctima, si bien el mal se le causará al afectar su libertad y autonomía.

En todo caso, más aún, en nuestro ordenamiento existen argumentos adicionales para no identificar las conductas analizadas con el delito de amenazas. El primero, toda vez que el delito de amenazas protege un bien jurídico colectivo —la seguridad pública—, entonces mal podrían identificarse estas conductas, ya que el acoso/ciberacoso en todas sus modalidades tutela la libertad y autonomía, no la seguridad colectiva.

El segundo, que "el acto debe tener un efecto colectivo, propio del terrorismo, y no simplemente consecuencias de temor a una persona o grupo reducido a causa de una acción."[254] Contrario a ello, el ciberacoso moral, aun cuando se puede ejecutar contra varias personas, no genera zozobra en el colectivo a partir de una acción, sino a partir de varias acciones dirigidas a los individuos.

Otro tanto se puede predicar para la injuria o la calumnia. Estos delitos suponen imputaciones deshonrosas o de una conducta típica. Para el acoso/ciberacoso, eso es apenas un elemento de lo que puede constituir una táctica acosadora/ciberacosadora, e incluso llegar a no ser totalmente identificable, aun cuando puedan ser considerados delitos de habla[255]. Es decir, a partir de la trasmisión de mensajes degradantes o de mensajes repetitivos no degradantes no necesariamente se estarán haciendo imputaciones deshonrosas o de una conducta típica. Así, por ejemplo, piénsese en mensajes constantes de un sujeto

---

[254] CRUZ BOLÍVAR, Leonardo. "Delitos contra la seguridad pública", en *Lecciones de derecho penal especial*, Vol. I, 3ª ed., Bogotá, Universidad Externado de Colombia, 2019, p. 652, quien además consigna referencias jurisprudenciales sustentado que así lo ha entendido la Corte Suprema de Justicia, Sala de Casación Penal (auto del 3 de agosto de 1989, M.P.: Jorge Carreño Luengas y auto del 29 de marzo de 1989, M.P.: Jaime Giraldo Ángel).

[255] Sin embargo, VILLACAMPA ESTIARTE. *Stalking y derecho penal, cit.,* p. 77 sugiere dejar de lado esa identificación sobre el *stalking* y considerarlo "más un delito de hechos que de palabras."

dirigidos a una mujer señalando sus despampanantes atributos físicos. Aquí, contrario a señalar una deshonra, se está exaltando a la víctima. Empero, al realizar de forma constante estos señalamientos, se estará afectando su libertad y autonomía cibernética para desenvolverse en el ciberespacio sin este tipo de intromisiones. Al final, estos mensajes podrían causarle un temor razonable.

Las comunicaciones pueden ser incluso mensajes sin contenido, con lo que se puede predicar su calidad de delito comunicativo, como la injuria o la calumnia lo son, pero no habrá imputaciones, empero aun así habrá desvalor merecedor de sanción. Piénsese en el caso "Momo" o de "La Ballena Azul", en donde las comunicaciones son amenazantes, pero no son imputaciones deshonrosas.

Lo anterior evidencia que el acoso moral y el ciberacoso moral se componen de varias tipologías conductuales cuyo elemento distintivo de las demás conductas es la combinación reiterativa y persistente que llegan a doblegar la voluntad de la víctima. Es solo cuando el acecho es permanente en el acoso predatorio o cuando las comunicaciones degradantes, humillantes o envilecedoras son reiterativas en el ciberacoso, o cuando existe una combinación de métodos de acoso o de ciberacoso (se persigue físicamente y se envían comunicaciones análogas; se realizan fotomontajes y se trasmiten mensajes degradantes) que es posible hablar de un "patrón de conducta" o "curso de conducta" que hace relevante esos hechos para la tipología criminal de acoso/ciberacoso.

En este sentido, la exclusión de la adecuación del acoso/ciberacoso moral con otros tipos penales señala que el acoso/ciberacoso moral se compone de varias conductas, que limitan o se superponen con otros delitos, pero que no comportan relevancia a menos que sean repetitivos y reiterativos.

Así, desde la perspectiva jurídica, se podrá debatir y se podrán adecuar los ordenamientos jurídicos a diferentes técnicas legislativas o formas de sanción, como será que consagren la conducta con el requisito del resultado (que la víctima tema o se altere su forma de vida) o de peligro (que la víctima potencialmente tema o potencialmente altere su forma de vida[256]); o consagren la conducta como subsidiaria (con lo que si se acredita otro delito que se haya superpuesto a la conducta acosadora/ciberacosadora deberá sancionarse ese otro delito) o como autónoma a los demás delitos (con lo que deberán operar las reglas concursales, salvaguardando a través de alguna fundamentación de desvalor el *non bis in*

[256] Sobre ello, consideramos más adecuado exigir el resultado jurídico de peligro, ponderando la aptitud del delito para menoscabar la libertad y autodeterminación del sujeto pasivo, tomando como referencia no a la víctima concreta (pues puede que la campaña no tenga efecto sobre ella por ostentar un umbral alto de resistencia), sino sobre una persona media colocada en la misma situación.

ídem[257]). Lo que es cierto es que toda conducta acosadora /ciberacosadora *debe ser* repetitiva y persistente, ya sea a través de una sola tipología conductual o a través de la combinación de varias de ellas, de forma directa o por medio de la instrumentalización o colaboración de terceros.

Con todo, esta interpretación puede chocar con la adecuación al tipo penal de hostigamiento consignado en el artículo 134B del Código Penal, ya que ese tipo penal sanciona promover o instigar a otros a que ejecuten actos, conductas o comportamientos constitutivos de hostigamiento, orientados a causarle daño físico o moral a una persona, grupo de personas, comunidad o pueblo en razón de su raza, etnia, religión, nacionalidad, ideología política o filosófica, sexo u orientación sexual, o discapacidad y demás razones de discriminación. Empero, tal choque es aparente, ya que el delito de hostigamiento se diferencia de la conducta de acoso y de ciberacoso moral estricto en diversos niveles.

En primer lugar, el tipo penal de hostigamiento es expresamente subsidiario, con lo que, si se adopta una fórmula para el acoso/ciberacoso que no lo sea, entonces nunca se superpondrán.

En segundo lugar, el delito de hostigamiento consiste en promover o instigar actos de hostigamiento y hemos visto como en el ciberacoso la automatización permite la repetición y persistencia del hostigamiento, sin que haya existido instigación o promoción frente a terceros.

En tercer lugar, el tipo de hostigamiento está vinculado a unos elementos normativos relacionados con la discriminación (es, de hecho, un instrumento antidiscriminación), lo que puede no concurrir en actos de acoso o de ciberacoso en donde no exista una motivación discriminadora por parte del agente; piénsese, en el acoso de acecho, en la predadora femenina que busca vigilar a su pareja masculina, o en el acoso/ciberacoso moral de los casos “Momo” o “La Ballena Azul”, donde lo que se vislumbra es un comportamiento abusivo y no discriminatorio en contra de los menores.

En cuarto lugar, el tipo de hostigamiento es de peligro abstracto y se consuma solo con la promoción o instigación, sin necesidad de que nadie atienda los actos de hostigamiento promovidos o instigados, mientras que para generar relevancia penal para el acoso o el ciberacoso en casos en que se inviten a terceros a

[257] Al respecto, es posible predicar el concurso de delitos así las conductas se superpongan en cuanto que el acoso/ciberacoso no comporta identidad de bien jurídico con los otros delitos superpuestos. Así, por ejemplo, un agente puede desplegar diversas tipologías conductuales de acoso/ciberacoso que impliquen amenazas, injurias y otras conductas no punibles autónomamente, debiendo responder concursalmente por los tres delitos, ya que la injuria lesionó la integridad moral, la amenaza puso en peligro a la seguridad pública y el acoso/ciberacoso lesionó la autonomía y libertad de la víctima.

hostigar es necesario que esos terceros, en efecto, desplieguen los actos de hostigamiento o ciberhostigamiento.

En quinto lugar, al ser un delito en contra de la vida y la integridad personal, será ese el bien jurídico que debe colocarse en peligro o lesionarse, lejos de la libertad o la autonomía, bienes jurídicos vinculados al acoso y al ciberacoso.

V. Tipologías conductuales y orientación jurídica

Un punto de gran debate sobre el acoso y el ciberacoso es el relacionado con sus tipologías conductuales. En concreto, sobre si cada una de estas formas de acoso psicológico conlleva sus propias tipologías y sobre si cada una de esas tipologías son la esencia del acoso.

Sobre lo primero, ya hemos adoptado una posición en la reseña de las tipologías acosadoras y ciberacosadoras, en el sentido de señalar que, dada la propia naturaleza modal de los medios empleados —análogos o cibernéticos—, podemos sostener que existen modalidades puras de acoso, modalidades puras de ciberacoso y modalidades mixtas, en donde es posible adecuar la conducta análoga o cibernética a dicha tipología.

Así, sostuvimos que la vigilancia electrónica es solo posible en el ciberacoso (predatorio o moral como medio de hostigamiento), mientras que la búsqueda de cercanía física es propia del acoso de acecho (exclusivo del acoso/ciberacoso predatorio). A su vez, la comunicación con la víctima es posible tanto por medios análogos como electrónicos.

Con lo anterior se hace evidente que las tipologías conductuales *no es lo determinante* para poder conceptualizar y diferencia entre acoso físico y acoso cibernético. Estas tipologías se comportan como *orientaciones jurídicas* con miras a la concreción del principio de tipicidad estricta. De ahí que varios ordenamientos jurídicos, como el español, hayan optado por la lista casuística de situaciones (tipológicas) que nos permiten hablar de “acoso” o de “*stalking*”. Dichas orientaciones son herramientas de hermenéutica jurídica, más no son los elementos que permiten fundamentar la existencia de un acoso o ciberacoso, ni la diferencia entre estos dos conceptos.

Contrario a ello, como se ha fundamentado, lo que nos permite hablar de acoso o de ciberacoso no es que exista una comunicación con la víctima o que se vigile o que se busque su cercanía física. Lo que hace a esos hechos acoso o ciberacoso es el establecimiento de un curso de conducta que implique una campaña de persecución (acoso/ciberacoso predatorio) o de degradación (acoso/ciberacoso moral).

Más aún, por ello es por lo que algunos ordenamientos no acuden a la casuística —el italiano, por ejemplo— y solo señalan el requisito de la sistematicidad. Así mismo, también por ello es por lo que algunos ordenamientos introducen una cláusula abierta para señalar que también es acoso o ciberacoso conductas por fuera de las tipologías conductuales, pero que cumplan con el patrón de conducta.

Por todo lo anterior, nuestra opinión es que las tipologías sirven de criterios orientadores de la tipicidad y de la interpretación jurídica, más no como elementos determinantes de la naturaleza de lo que es una conducta de acoso o de ciberacoso[258].

VI. Etiología multifactorial del (ciber)acoso moral estricto

En el acápite pertinente de este trabajo, se realizó un barrido de las teorías etiológicas más prevalentes en la explicación de las causas de la desviación acosadora y ciberacosadora. Allí, se repasó la teoría psicológica —en alguna época la única teoría explicativa de este fenómeno criminal—, la teoría del aprendizaje social, la teoría de la elección racional y la teoría de las actividades rutinarias.

A. Crítica a la teorías reseñadas

1. La teoría psicológica como reducción del fenómeno a criterios biológicos

Así, tenemos para nosotros que cualquier posición que busque fundamentar de forma exclusiva las causas del ciberacoso en la teoría psicológica, carecerá de profundidad y amplitud para poder explicar todas las formas en que el acoso psicológico se desenvuelve. En efecto, la teoría psicológica, considerando que se fundamenta en el trastorno mental del agente la existencia de la conducta, solo lograría dar una explicación parcial al acoso y ciberacoso predatorio, en cuanto que esa es una de las modalidades que comportan algún tipo de obsesión afectiva del agente con la víctima; y logrará una nula explicación en relación con el acoso y ciberacoso moral, donde ese tipo de obsesión no se presenta. En efecto, el ciberacosador moral no se comporta de dicha manera, en cuanto que las más de las veces es un sujeto solitario que ataca sin moverse de la terminal electrónica, es decir, sin querer cercanía física o amorosa con la víctima, sin ser motivado por una obsesión afectiva, producto de un trastorno mental o no.

[258] En cuanto a la fórmula de tipificación, nos inclinamos por una descripción abierta, del estilo del delito de acoso sexual en Colombia, en cuanto que las listas cerradas dejan por fuera el constante avance de la tecnología y se presentan muy casuísticas.

En este orden de idas, estas aproximaciones psicológico-psiquiátricas deben tomarse con beneficio de inventario, ya que no solo porque se hayan identificado algunos casos que encuadran en el patrón se puede afirmar que ello es así para todos los demás. Un paso más allá, se pueden denunciar estas corrientes como conformistas, ya que reducen el problema del fenómeno de la desviación a criterios biológicos, lo que ya la historia demostró pueden ser abusados para promover grandes afrentas a los derechos humanos.

2. La teoría del aprendizaje social como forma de explicar ciertos tipos de acoso

En relación con la teoría del aprendizaje social, debemos decir que la adoptamos, ya que comporta elementos adecuados para dar explicación a la forma en cómo el ciberacosador moral se manifiesta. En este sentido, nótese que no sostenemos que sea la teoría adecuada para explicar todas las formas de acoso y de ciberacoso. Por el contrario, consideramos que este entendimiento arroja luces sobre el comportamiento del acoso moral, en especial del acoso moral estricto u hostigamiento.

Lo anterior toda vez que, según la teoría del aprendizaje social, es posible sostener que, si una víctima responde al curso de conducta intimidante u hostigador del ciberacosador, entonces el ciberacosador habrá recibido un refuerzo positivo para seguir ejecutando la conducta, ya que logró una reacción en su víctima, sea ella positiva o negativa. En este sentido, lo recomendable frente a los ciberacosadores es ignorarlos, no empezar una discusión directa y en vez de ello denunciarlos o reportarlos. De lo contrario se estaría motivando la repetición y formación del curso de conducta, ya que el desespero o el desasosiego por recibir el ataque es el combustible para continuar con la degradación propia del ciberacosador moral.

3. La teoría de las actividades rutinarias como explicación de la racionalidad de la conducta en el ciberespacio

Hasta hoy, la teoría más aceptada para dar explicación al acoso y ciberacoso moral es la teoría de las actividades rutinarias. A nuestro entender, dicha aceptación es correcta, ya que esta teoría, junto con la teoría de la elección racional, da cuenta de la forma racional y oportunista en que los criminales ejecutan sus conductas.

Con todo, más allá, consideramos que la teoría de las actividades rutinarias es excepcional a la hora de dar explicación a las causas que de la cibercriminalidad de la Web 2.0, en especial, de la cibercriminalidad social que nos permite considerar al ciberacoso moral como un verdadero cibercrimen estricto o propio.

Como se ha explicado, la Web 2.0 supuso un revolcón en la forma en cómo usamos el Internet y la manera en que nos relacionamos socialmente en el ciberespacio, generando nuevos ámbitos de desarrollo a la par que se creaban nuevos espacios de ciberdelincuencia. Es decir, en términos de la teoría comentada, el cambio de las actividades diarias o rutinarias de los asociados respecto de la Red, esto es, la nueva forma de desarrollarnos como ciudadanos-usuarios digitales, implicó una ruptura de formas sociales grandísima, asimilable a lo analizado por COHEN y FELSON en la época de la posguerra, cuando nada de las formas sociales rutinarias de esa época se parecía a las formas sociales rutinarias previas a las guerras o del período de entreguerras.

En esos tiempos, fue el *boom* económico que llevó a las familias a adquirir bienes domésticos, portátiles pero funcionales —televisores, tostadoras, cafetera—, lo que generó la oportunidad para los delincuentes. Después, cuando ya las casas debían permanecer vacías durante el día —padre y madre trabajaban, y chicos a la escuela—, esta actividad rutinaria generó otra oportunidad para los delitos. Los avances tecnológicos, las más de las veces, vienen aparejados con nuevas oportunidades delictivas, como sucedió con los cajeros automáticos, ahora lugares propicios para el asalto a mano armada.

El Internet fue uno de aquellos avances tecnológicos que simplemente generó disrupción en toda forma de actividad rutinaria para adecuarse a una nueva rutina social, rica en oportunidades delictivas. Los ejemplos más claros de ello han venido desde la cibercriminalidad económica: entre más transacciones se den en el Internet, mayor oportunidad habrá para el fraude. Como lo señala GRABOSKY, todas las situaciones delictivas propiciadas por el Internet ponen de manifiesto que el ciberespacio tiene la misma función que una parada de bus, el patio a la salida del colegio o la discoteca en la Zona Rosa: son todos lugares propicios de encuentros entre agresores potenciales y víctimas adecuadas[259].

En el ámbito criminal del ciberacoso moral, varios ejemplos ponen de manifiesto la adecuación de la teoría de COHEN y FELSON. Piénsese en los menores como víctimas adecuadas sometidas en ausencia de guardianes capacitados. O en la publicación de información personal en Internet como manifestación de la libertad cibernética y el desarrollo personal, pero a la vez como oportunidad y motivación para el agresor, que encuentra todos los insumos necesarios para desplegar su táctica proveídos por la propia víctima a la cual someterá.

El anonimato, la fácil y barata accesibilidad al ciberespacio o la gran probabilidad de lograr la impunidad son también motivadores eficaces para que los cibercriminales y ciberacosadores aprovechen las oportunidades delictivas

[259] GRABOSKY. "Virtual criminality: Old wine in new bottles?", *cit.,* p. 244.

brindadas por el ciberespacio. Por todo ello, adoptamos la teoría de la elección racional y de las actividades rutinarias como explicaciones adecuadas del fenómeno multifactorial que el ciberacoso moral es en las sociedades modernas.

Ahora, como lo reseñamos en el acápite pertinente, la teoría de las actividades rutinarias no está exenta de críticas. Las tres críticas realizadas por KREMLING y SHARP PARKER (cfr. *supra*, n. 218) son:

(i) *Si la teoría de las actividades rutinarias exige que para que se dé la oportunidad delictiva debe converger el espacio y el tiempo, ello no es posible en el ciberespacio, donde espacio y tiempo no convergen.*

Esta crítica no tiene en cuenta precisamente los efectos que la ubicuidad, deslocalización y distribución del ciberespacio tienen sobre la convergencia de espacio y tiempo. Como el espacio y el tiempo se contraen y relativizan en el espacio cibernético, la convergencia de estos elementos no depende de criterios físicos que permitan que en un lugar determinado (el suburbio) y a una hora determinada (la mañana) se den las condiciones para la oportunidad delictiva. Contrario a ello, esa convergencia en el ciberespacio es *continua*, nunca para, y solo depende de que (i) el usuario esté conectado y (ii) esté ejecutando la relación social (económica, personal, etc.) adecuada para el aprovechamiento del delincuente. En el caso del ciberacoso moral, no es necesario que sea determinado momento el que el usuario se conectó o que se haya conectado desde su casa o desde la universidad. Lo importante es que *comparte* el espacio-tiempo de la oportunidad delictiva (el ciberespacio deslocalizado, atemporal y distribuido).

(ii) *Sostienen las autoras que la ausencia de un guardián capacitado puede variar de agresor en agresor y de víctima en víctima, con lo que se quiere señalar que la teoría no puede explicar todas las formas criminales, puesto que los protagonistas son los que determinan el resultado de la interacción criminal.*

En nuestra opinión, la crítica es desenfocada, habida cuenta que la teoría de las actividades rutinarias quiere, de forma general, explicar porque se producen ciertos delitos que recogen ciertas características, como los tres factores mencionados (la presencia de un agresor motivado, la existencia de una víctima adecuada y la ausencia de un vigilante capacitado). Ahora, el éxito o el fracaso de una empresa criminal dependerán de mayores variables, como el nivel de capacitación de los guardianes o el nivel de satisfacción de un motivo para llevar al agente a realizar la conducta. De esta forma, es cierto que la ausencia de un guardián capacitado puede variar de caso en caso, empero, ello no obsta para explicar que, en determinados casos, como los de ciberacoso, el hecho se desarrolla y concreta porque los tres elementos de las actividades rutinarias

convergen de forma concreta en el ciberespacio. Con todo, puede que una empresa criminal de ciberacoso moral fracase por la adecuada preparación de un guardián, sin que ello obste para vislumbrar que la causa del ataque fue una motivación adecuada, una víctima propensa y (en este caso) el mal cálculo sobre la capacitación del guardián.

(iii) *Finalmente, sostienen que mal podría el agente calcular sobre beneficios o pérdidas del acto si los guardianes en el ciberespacio son invisibles (puesto que uno puede ver una reja en el espacio físico, pero no un firewall en el espacio virtual).*

Esta crítica también sufre falencias, ya que asume que en el espacio físico no existen guardianes invisibles, cuando lo cierto es que también existen: cámaras ocultas, sensores infrarrojos, alarmas. Por ello, el punto no debe enfocarse en el nivel de exposición de las medidas de seguridad, sino en la motivación del agente para, con base en su información disponible, emprender o no la actividad criminal. Es decir, el ciberespacio es un lugar lleno de oportunidades criminales, pero como en toda actividad relacionada con el aprovechamiento de una oportunidad, el resultado nos es desconocido desde el principio y solo avanzamos de acuerdo con la ponderación de la información disponible y de la información conseguida.

Por lo anterior, la crítica no desvirtúa la capacidad de la teoría de la elección racional y de la teoría de las actividades rutinarias de explicar los factores que el ciberespacio provee a las causas del cibercrimen social.

B. Otras teorías relevantes

Las cuatro teorías comentadas sirven para explicar varios aspectos o algunas facetas del fenómeno de la cibercriminalidad social y del ciberacoso moral. Sin embargo, de nuestra investigación surgen como adecuadas otras teorías que servirían para ilustrar acerca de la naturaleza multifactorial del ciberacoso.

Es decir, el ciberacoso moral no es solo producto de obsesiones psicológicas —con efectos de inimputabilidad en nuestro medio—, o del aprendizaje social que absorbe el agente cuando obtiene la reacción adecuada de la víctima, o la racionalidad del autor y la convergencia de factores que propician la oportunidad delictiva; a nuestro entender, podemos fundamentar, con base en dos teorías más, las causas de la existencia de este fenómeno criminal del siglo XXI: la teoría de transición de espacios y el concepto de ceremonias de degradación y de prejuicio social.

1. Teoría de la transición de espacios

Uno de los muchos efectos de la Revolución Tecnológica en nuestros medios es que generó la necesidad de configurar nuevas disciplinas científicas que lograran o intentaran precisamente la explicación de estos efectos en la sociedad. Así, a la par —o tal vez algunos lustros después— del surgimiento de la informática y de las ciencias de la computación, en las ciencias sociales también fueron surgiendo corrientes de estudio de la mutabilidad digital, un concepto que se funda en la idea de nuestro presente como mutantes digitales, esto es, como un resultado de unas interacciones de lo humano con lo tecnológico.

En esta línea, JAISHANKAR defiende la autonomía de la cibercriminología como un campo de estudio multidisciplinario autónomo en el cual concurren la criminología, la victimología, la sociología, las ciencias informáticas y las ciencias computacionales. Con el fin de desarrollar este campo de estudio, introdujo la teoría de la transición de espacios, con la que pretende explicar las causas que permiten la cibercriminalidad. Mediante dicha teoría, se busca explicar la naturaleza del comportamiento de los sujetos cuando lo manifiestan como acorde o no acorde al ordenamiento, tanto en el espacio físico como en el cibernético[260].

La teoría de la transición de espacios involucra el movimiento o tránsito de las personas de un espacio a otro, por ejemplo, de un espacio físico a uno cibernético, o viceversa. A partir de ello, la teoría sostiene que los sujetos se comportan diferente en cada uno de aquellos espacios, dadas las particularidades de estos[261].

Los postulados de la teoría son los siguientes[262]:

i. Sujetos con comportamiento criminal reprimido (en el espacio físico) tendrán una propensión a ejecutar crímenes en el ciberespacio, que de otra forma no cometerían dado su estatus y su posición social.

ii. La flexibilidad en la construcción de identidad, la disociación que provee el anonimato y la falta de disuasión en el ciberespacio, le proveen a los ofensores los medios para ejecutar cibercrímenes.

iii. El comportamiento criminal en el ciberespacio puede llegar a ser importado al espacio físico, a la vez que el comportamiento criminal en el espacio físico puede llegar a ser exportado al mundo cibernético.

---

[260] JAISHANKAR, K. “Expanding cybercriminology with an avant-garde anthology”, en JAISHANKAR K. (ed.). *Cybercriminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011, p. XXVII.

[261] JAISHANKAR, K. “Space transition theory of cybercrimes”, en SCHMALLEGER, Frank; PITTARO, Michael (eds.). *Crimes of the Internet*, Upper Saddle River, Prentice Hall, 2008, pp. 283 y ss.

[262] JAISHANKAR. “Space transition theory of cybercrimes”, *cit.,* pp. 292-293.

iv. Las aventuras intermitentes de los ofensores al ciberespacio y la propia naturaleza dinámica del espacio y tiempo en él les proveen a aquellos una válvula de escape.

v. Los desconocidos pueden asociarse en el ciberespacio para cometer crímenes en el mundo físico, mientras que los conocidos pueden asociarse en el mundo físico para cometer delitos en el ciberespacio.

vi. Sujetos pertenecientes a sociedades cerradas son más propensos a cometer delitos en el ciberespacio de sus pares pertenecientes a sociedades más abiertas.

vii. El conflicto y choque que se genera entre los valores que imperan en el espacio físico con los valores que gobiernan en espacio cibernético puede llevar a la comisión de cibercrímenes.

Con esta teoría se pretende explicar cómo el ambiente (el *locus*) genera una influencia determinante en la desinhibición de los sujetos para ejecutar conductas antijurídicas. En este caso, el ciberespacio se comporta como un territorio de neutralidad y libertad donde los juicios sobre lo desviado o no de una conducta caminan por una delgada línea que se debate entre la libertad en la red o la necesidad de regulación para gestionar conflictos y evitar daños.

En relación con los ciberacosadores morales, parece adecuado asumir que el solitario agente ataca y hostiga a víctimas vulnerables —menores, mujeres, novatos— motivado porque la disociación que existe entre el ciudadano de carne y hueso y el usuario virtual que interactúa bajo seudónimos en espacios virtuales le permite desplegar un comportamiento hamletiano, es decir, de ser y no ser al mismo tiempo. El desdoblamiento de personalidad (que sucede en algún momento del tránsito espacial) le permite al agente mantener un estatus moral frente a sus relaciones físicas, y al mismo tiempo, desembarazarse de las restricciones que mantener ese estatus moral le impone, pero ahora en el espacio cibernético, lejos de la mirada y juicio de sus contrapartes físicas.

2. Ceremonias de degradación y prejuicio social

Por otra parte, en los años sesenta, a partir de un contexto dominado por la sociología de la desviación que no cesaba su implacable crítica en contra del positivismo, GARFINKEL presentó su concepto de las ceremonias de degradación. “Todo trabajo comunicativo entre personas, en donde la identidad pública de un actor es transformada en algo visto como menor dentro del esquema

local de tipos sociales, debe ser llamado como *ceremonia de degradación de estatus*."[263]

Lo anterior quiere decir que dentro de las interacciones sociales —el concepto de GARFINKEL sería adoptado por el trabajo del interaccionismo simbólico en el contexto de las teorías de la desviación de los años sesenta— los actores realizan determinados rituales (que no por ello siempre formales[264]) en los cuales se eleva una denuncia pública (por el denunciante que adopta y refleja los valores dominantes) en contra de otro actor, ante la participación activa o pasiva de terceros (llamados testigos), y cuyo fin es la constitución de un estatus totalizador, tanto para el grupo —en función del refuerzo de la solidaridad de grupo— como para el degradado, cuya exclusión debe ser diáfana, mostrándose como diferente y por tanto condenado a la otredad.

Para que la ceremonia de degradación de estatus tenga éxito es necesario que se presenten determinadas circunstancias rituales[265].

En un primer lugar, el actor y el suceso adelantado por el actor deben ser percibidos como "anormales" o "desviados" de la corriente general (*mainstream*).

En segundo lugar, el actor y el acto deben formar parte de una categoría de actores o de actos que no sea posible ser explicada por alguna idea de accidente, casualidad o excepcionalidad (es decir, no puede haber "justificación social" del suceso ni de su titular en ojos del resto del grupo).

En tercer lugar, los testigos —que pueden comportarse activamente como jurados de la ceremonia— deben analizar al actor y a su suceso en relación con ellos mismos, pero con el énfasis de precisamente de "no ser él como somos nosotros." Son los testigos los primeros en manifestar el sentimiento social de indignación, que es el punto de partida para iniciar la ceremonia y el punto de llegada para satisfacer el deseo de exclusión.

En cuarto lugar, el acusador —el denunciante— debe ser visto como un representante público que representa las cualidades y los valores adoptados por la mayoría grupal. Éste sujeto, al estilo del delegado de la acusación estatal (según GARFINKEL, el proceso penal es la ceremonia de degradación por excelencia), no actúa en interés propio, sino por el interés público, "el interés de todos", siendo

---

[263] GARFINKEL, Harold. "Conditions of successful degradation ceremonies", en *American Journal of Sociology*, Vol. 61, No. 5, Chicago, University of Chicago Press, 1959, p. 420. (*Trad. del Aut.*).

[264] ESCOBAR BELTRÁN, Samuel. "Ceremonias de degradación y debates actuales sobre el castigo", en *Revista Contemporánea de Derecho Penal*, No. 51, Bogotá, Legis, abril-junio de 2015, p. 137.

[265] LARRAURI, Elena. *La herencia de la criminología crítica*, 2ª ed., Ciudad de México, Siglo Veintiuno, 2009, p. 41; más detalladamente, GARFINKEL. "Conditions of successful degradation ceremonies", *cit.,* pp. 422-423.

entonces elemento crucial del éxito de la ceremonia de degradación que exista identificación moral entre el denunciante y los testigos-jurados.

En quinto y último lugar, el denunciado debe ser "extrañado", es decir, debe declararse que él ni sus valores tienen nada que ver con los valores de la comunidad (aquí constituida por el denunciante y el jurado), teniendo que ser ritualmente separado de la comunidad como un "extranjero".

Este tipo de razonamiento en concordancia con la teoría de selección de la víctima mediante el prejuicio social explica como en algunos casos de ciberacoso moral lo que subyace al ataque es una ceremonia de degradación en la cual la víctima ha sido escogida para ejercer sobre ella un uso de la violencia excluyente. Recuérdese el caso del estudiante Sergio Urrego, sometido al acoso moral de las directivas del colegio, excluido por su condición de homosexual.

En relación con la teoría de la selección de la víctima por prejuicio, se ha sostenido[266] que este tipo de criminalidad es producto de su contexto, es decir, es síntoma y resultado de una sociedad prejuiciosa. Así, los procesos de definición de lo desviado o antisocial pasan por lo que sea de interés para las jerarquías de poder, que en virtud de sus relaciones dominantes instrumentalizan el lenguaje —y por esta vía el derecho penal— para mantener el *statu quo*.

Los prejuicios sociales encuentran vital relevancia en la explicación de la violencia de género en contra de la mujer y en contra de los grupos con orientaciones o identidades sexuales diversas. En efecto, el agente despliega lo usos de la violencia —jerarquizadora o excluyente— basado en su percepción de justicia o de restablecimiento del valor del grupo. En estos contextos, los conflictos surgen cuando se ha afrentado al (des)valor prejuicioso, como cuando se cuestiona la "propiedad" de un hombre sobre la su mujer o se pone en duda el posicionamiento del hombre heterosexual, casos en los que se recurre a la violencia jerarquizadora o excluyente porque para ser considerado heterosexual no basta la atracción con el género opuesto, sino que también se hace necesario controlar, reprimir y degradar —mediante ceremonias rituales— a la homosexualidad[267].

En este orden de ideas, estos conceptos presentan valor para explicar etiológicamente el ciberacoso, en cuanto que muchas veces el agente escoge a su víctima al azar, pero dentro del marco de su prejuicio, con el fin de degradar la posición moral de la víctima. Para ello, se hace valer de los prejuicios del resto del

---

[266] ESCOBAR BELTRÁN, Samuel. "Del odio al prejuicio: Reflexiones sobre la subjetividad y su prueba en instrumentos penales antidiscriminación", en *Estudios socio-jurídicos*, Vol. 18, No. 2, Bogotá, Colegio Mayor de Nuestra Señora del Rosario, julio 2016, pp. 182-186.

[267] ESCOBAR BELTRÁN, Samuel. "Ceremonias de degradación y debates actuales sobre el castigo", *cit.,* p. 144. ÍD. "Del odio al prejuicio: Reflexiones sobre la subjetividad y su prueba en instrumentos penales antidiscriminación", *cit.,* p. 183.

grupo y conforma la denuncia pública frente a su degradado para generar la indignación social que le permitirá hostigar al sujeto pasivo.

Las mujeres y los grupos con orientaciones e identidades sexuales diversas son las víctimas más adecuadas para degradar ritualmente, ya que los prejuicios sobre estos grupos sociales están profundamente arraigados en el colectivo. Como lo demuestra el informe citado de Reporteros Sin Fronteras, las mujeres periodistas, y en especial las mujeres periodistas de investigación o deportivas, son las que más sufren el ciberacoso de parte de los usuarios de la Red, ya que rompen con el rol de género a ellas establecidas (¿desde cuándo una mujer puede saber de fútbol?).

La participación de jurado en las ceremonias de degradación ciberacosadoras es fundamental, porque las más de las veces, al ser un rasgo que el Internet promueve —la transición, desdoblamiento y disociación del anonimato—, el testigo se transformará de un espectador a un denunciante-acosador activo. Como se ha dicho, el ciberespacio facilita la invitación a terceros para unirse al ciberacoso, siendo ello un acontecimiento perfectamente explicado en el contexto de las ceremonias de degradación, donde a como dé lugar —de ahí su carácter totalizador señalado por GARFINKEL— el otro debe ser excluido, siendo el hostigamiento repetitivo y la intimidación constante métodos más que eficaces para la consecución del objetivo.

En este sentido, el prejuicio social y las ceremonias de degradación sirven para iluminar cuál es la causa que lleva a un ciberacosador a degradar, intimidar y hostigar a su víctima.

Conclusiones

Ha sido el objetivo de este trabajo, en primer lugar, determinar la naturaleza de los cibercrímenes para, en segundo lugar, fundamentar la sistematización y conceptualización de los diversos tipos de acoso, en especial del acoso moral y del ciberhostigamiento como una nueva forma cibercriminal necesitada de regulación en el ordenamiento jurídico colombiano, al hacerse palpable el carácter lesivo que esa conducta ostenta a partir de las nuevas dinámicas de las relaciones sociales cibernéticas.

En concreto, arribamos a las siguientes conclusiones:

1. El ciberespacio y el Internet son elementos determinantes de la vida individual y social que diseñan y moldean la forma en que nos desarrollamos y la forma en que nos comunicamos intersubjetivamente.

2. Por ello, a la par de los valores y transformaciones positivas que esos ambientes cibernéticos han traído, han surgido también formas de criminalidad nunca vistas, nuevas en su naturaleza o evolucionadas en su concepción, que han establecido la necesidad de gestión jurídica a partir de su identificación y sanción.

3. Así, es necesario ampliar el concepto de criminalidad vinculada a las nuevas TIC, al Internet y al ciberespacio, desplazando la visión purista y restrictiva de la criminalidad informática y en su lugar desarrollar un entendimiento de una criminalidad cibernética más amplia que incluya, como debe ser, a las nuevas conductas informáticas junto con las viejas conductas que se aventajan de las TIC y las conductas también clásicas que evolucionan en sus injustos típicos a partir de las nuevas posibilidades de la interacción cibernética y social.

4. La identificación de las características lesivas de esta nueva criminalidad cibernética es esencial con el objeto de gestionar los mayores retos y problemas que estos actos desviados proponen a las autoridades estatales, en el sentido que el conocimiento de lo que caracteriza a esta criminalidad serán o deberán ser los focos de atención a gestionar.

5. Debe aceptarse que existen diversos tipos de acoso, que no todos ellos son criminales y que algunos pueden llegar a distanciarse, empero, todos ellos comportan dos elementos comunes que de no concurrir no se podrá sostener su naturaleza como comportamiento acosador: (i) el riesgo psicológico para la víctima y (ii) la repetición y persistencia de la conducta.

6. Fuera de estos dos elementos comunes, las diversas conductas de acoso empiezan a tomar sus propias características incluyentes que les otorgan autonomía y distinción, las cuales devienen de lo que llamamos “hábitat o entorno social”, o lo que es lo mismo, espacio concreto de desenvolvimiento de relaciones sociales: relaciones afectivas, relaciones sexuales, relaciones laborales, relaciones escolares, relaciones contractuales o relaciones interpersonales.

7. Algunos de estos hábitats o entornos sociales, además, se encuentran influenciados por el medio cibernético de forma intensa, al punto que le pueden otorgar a ciertas conductas autonomía cibernética, ya que de ahí surgen nuevas características criminales, más disvaliosas, necesitadas de gestión. Así sucede con el acoso moral cibernético o el ciberhostigamiento

8. Si la influencia cibernética no es tan intensa y más bien se ha acudido a las herramientas del ciberespacio como forma de reforzar el acto físico, entonces la conducta no será puramente cibernética ni autónoma, sino una nueva forma extensiva en que se está ejecutando la conducta clásica. Así sucede con el ciberacoso predatorio, que es una táctica extensiva de refuerzo del acoso predatorio físico (o viceversa).

9. En Colombia no existen conductas criminales de acoso, más allá del acoso sexual, ni de hostigamiento degradante, más allá de conductas clásicas insuficientes como la injuria, la calumnia, las amenazas, el constreñimiento ilegal o el hostigamiento discriminatorio. Por ello, antes de la necesaria legislación penal, se hace necesario se ahonde en los conceptos pre-jurídicos de los fenómenos con miras a tener las bases y la información adecuada para delinear la política criminal.

Bibliografía

Doctrina

ABOSO, Gustavo Eduardo. *Derecho penal cibernético,* Buenos Aires, B de F, 2018.

ALONSO DE ESCAMILLA, Avelina. "El delito de stalking como nueva forma de acoso. El 'cyberstalking' y nuevas realidades", en RIQUERT, Marcelo A. (coord.). *Ciberdelitos*, 2ª ed., Buenos Aires, Hammurabi, 2019.

ÁLVAREZ ÁLVAREZ, Suleima. *Consideraciones sobre el nuevo delito de acoso*, San Cristóbal de la Laguna, Universidad de la Laguna, 2016-2017.

ARBELÁEZ GIRALDO, Andrea. "El ciberespacio y el problema de la realidad virtual", en *Revista de filosofía UIS*, Vol. 16, Bucaramanga, Universidad Industrial de Santander, julio-diciembre de 2017.

BENAVIDES MORALES, David. "Delitos contra la libertad, integridad y formación sexuales", en CASTRO CUENCA, Carlos G. (coord.). *Manual de derecho penal parte especial*, T. I, 2ª ed., Bogotá, Temis, Universidad del Rosario, 2018.

BOCIJ, Paul; McFARLANE, Leroy. "Seven fallacies about cyberstalking", en *Prison Service Journal*, No. 149, Gloucestershire, Center for Crime and Justice Studies, 2003.

CASTRO SANTANDER, Alejandro; RETA BRAVO, Cristina. *Bullying blando, Bullying duro y ciberbullying. Nuevas violencias y consumos culturales*, Santa Fe, Homo Sapiens, 2013.

CLOUGH, Jonathan. *Principles of cybercrime*, Cambridge, Cambridge University Press, 2010.

CÓRDIBA ANGULO, Miguel. "Delitos contra la integridad moral", en *Lecciones de derecho penal parte especial*, V. I, Bogotá, Universidad Externado de Colombia, 2019.

CRISAFI, Denise N.; MULLINS, Alyssa R.; JASINSKI, Jana L. "The rise of the virtual predator: technology and the expanding reach of intimate partner abuse", en NAVARRO, Jordana N.; CLEVENGER, Shelly; MARCUM, Catherine D. (eds.). *The intersection between intimate partner abuse, technology and cybercrime*, Durham, Carolina Academic Press, 2016.

CRUZ BOLÍVAR, Leonardo. "Delitos contra la seguridad pública", en *Lecciones de derecho penal especial*, Vol. I, 3ª ed., Bogotá, Universidad Externado de Colombia, 2019.

ELLISON, Louise; AKDENIZ, Yaman. "Cyberstalking: The regulation of harassment on the Internet", en *Criminal Law Review*, diciembre de 1998.

ESCOBAR BELTRÁN, Samuel. "Ceremonias de degradación y debates actuales sobre el castigo", en *Revista Contemporánea de Derecho Penal*, No. 51, Bogotá, Legis, abril-junio de 2015.

ESCOBAR BELTRÁN, Samuel. "Del odio al prejuicio: Reflexiones sobre la subjetividad y su prueba en instrumentos penales antidiscriminación", en *Estudios socio-jurídicos*, Vol. 18, No. 2, Bogotá, Colegio Mayor de Nuestra Señora del Rosario, julio 2016.

FUKUYAMA, Francis. *The End of History and the Last Man*, New York, The Free Press, 1992.

GARCÍA GUILABERT, Natalia. *El ciberacoso. Análisis de la victimización de menores en el ciberespacio desde la teoría de las actividades rutinarias*, Buenos Aires, B de F, 2017.

GARFINKEL, Harold. "Conditions of successful degradation ceremonies", en *American Journal of Sociology*, Vol. 61, No. 5, Chicago, University of Chicago Press, 1959.

GARZÓN ROA, Andrés. "Delitos contra la libertad individual y otras garantías", en CASTRO CUENCA, Carlos (coord.). *Manual de derecho penal parte especial*, T. I, 2ª ed., Bogotá, Temis, Universidad del Rosario, 2018.

GRABOSKY, Peter N. "Virtual criminality: old wine in new bottles?", en *Social & legal studies*, No. 10:2, Thousand Oaks, SAGE, 2001.

HALDER, Debarati; JAISHANKAR, K. "Online social networking and women victims", en JAISHANKAR, K. (ed.). *Cybercriminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011.

HARARI, Yuval Noah. *From animals into Gods*, Scotts Valley, Create Space, 2012.

HOFFMEISTER, Thaddeus. "Legislative reactions", en NAVARRO, Jordana N.; CLEVENGER, Shelly; MARCUM, Catherine D. (eds.). *The intersection between intimate partner abuse, technology and cybercrime*, Durham, Carolina Academic Press, 2016.

JAISHANKAR, K. "Expanding cybercriminology with an avant-garde anthology", en JAISHANKAR K. (ed.). *Cybercriminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011.

JAISHANKAR, K. "Space transition theory of cybercrimes", en SCHMALLEGER, Frank; PITTARO, Michael (eds.). *Crimes of the Internet*, Upper Saddle River, Prentice Hall, 2008.

KILEL, Beatrice. *Cyberstalking: Electronic harassing,* Frederick, Zapphire Publishing, 2014.

KREMLING, Janine; SHARP PARKER, Amanda M. *Cyberspace, cybersecurity and cybercrime*, Thousand Oaks, SAGE, 2018.

LARRAURI, Elena. *La herencia de la criminología crítica*, 2ª ed., Ciudad de México, Siglo Veintiuno, 2009.

LEINER, Barry M. *et ál*. *A brief history of Internet*, Internet Society, 1997.

LORA MÁRQUEZ, Marian. *Estudio jurídico doctrinal del delito de acoso o stalking*, Sevilla, Universidad Internacional de la Rioja, 2017.

LORENZO BARCENILLA, Silvia. *Stalking. El nuevo delito de acecho del art. 172 ter del Código Penal*, Barcelona, Universidad Oberta de Catalunya, 2015.

MELOY, J. Reid; GOTHARD, Shayna. "Demographic and clinical comparison of obsessional followers and

offenders with mental disorders", en *American Journal of Psyquiatry*, No. 152:2, American Psychiatric Association, February 1995.

MIRÓ LLINARES, Fernando. *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons, 2012.

MISHRA, Alok; MISHRA, Deepti. "Cyberstalking: A challenge for web security", en JANCZEWSKI, Lech J.; COLARIK, Andrew M. *Cyberwarfare and cyberterrorism*, London, IGI Global, 2008.

MULLEN, Paul; PATHÉ, Michele; PURCELL, Rosemary. *Stalkers and their victims*, Cambridge, Cambridge University Press, 2000.

MULLEN, Paul; PATHÉ, Michele; PURCELL, Rosemary; STUART, Geoffrey W. "Study of stalkers", en *American Journal of Psychiatric*, No. 156:8, American Psychiatric Association, August 1999.

NAVARRO, Jordana N. "Cyberabuse and cyberstalking", en NAVARRO, Jordana N.; CLEVENGER, Shelly; MARCUM, Catherine D. (eds.). *The intersection between intimate partner abuse, technology and cybercrime*, Durham, Carolina Academic Press, 2016.

NAVARRO RODRÍGUEZ, Miguel; BARRAZA MACÍAS, Arturo. "Redes sociales y uso patológico del Internet: síntomas y efectos negativos en jóvenes", en *XI Congreso Nacional de Investigación Educativa*.

NEWBURN, Tim. *Criminology*, 2ª ed., London, Routledge, 2013.

OCAMPO GAVIRIA, José Antonio, *et ál*. "La industrialización y el intervencionismo estatal (1945-1980)", en OCAMPO GAVIRIA, José Antonio. *Historia económica de Colombia*, Bogotá, Fedesarrollo, 2007.

PATHÉ, Michele; MULLEN, Paul. "The impact of stalkers on their victims", en *British Journal of Psychiatric*, No. 174, Royal College of Psychiatrist, 1997.

PÉREZ KASPARIAN, Sara. *Manual de criminología*, Ciudad de México, Porrúa, 2014.

PÉREZ PINZÓN, Álvaro Orlando; PÉREZ CASTRO, Brenda Johanna. *Curso de criminología,* 7ª ed., Bogotá, Universidad Externado de Colombia, 2006.

PITTARO, Michael L. "Cyberstalking: typology, etiology and victims", en JAISHANKAR, K. (ed.). *Cybercriminology. Exploring Internet crimes and criminal behavior*, Boca Ratón, CRC Press, 2011.

POSADA MAYA, Ricardo. *Delitos contra la vida y la integridad personal*, T. II, Bogotá, Ibáñez, Universidad de los Andes, 2015.

POSADA MAYA, Ricardo. *Los cibercrímenes: un nuevo paradigma de criminalidad*, Bogotá, Ibáñez, Universidad de los Andes, 2017.

REYES ECHANDÍA, Alfonso. *Criminología*, 8ª ed., Bogotá, Temis, 2003.

REYES ECHANDÍA, Alfonso. *Derecho penal*, 11ª ed., Bogotá, Temis, 2017.

RIQUERT, Marcelo A. “Repensando cómo funcional la ley penal en el ciberespacio”, en RIQUERT, Marcelo A (coord.). *Ciberdelitos,* 2ª ed., Buenos Aires, Hammurabi, 2019.

ROYAKKERS, Lambers. “The Dutch approach to stalking laws”, en *Berkeley Journal of Criminal Law,* Vol. 3, No. 1, Berkeley University of California, 2000.

SAIN, Gustavo. “Internet, el cibercrimen y la investigación criminal de delitos informáticos”, en SAIN, Gustavo, AZZOLIN, Horacio. *Delitos informáticos*, Buenos Aires, Montevideo, B de F, 2017.

SAMPEDRO ARRUBLA, Camilo. “Delitos contra la libertad individual y otras garantías”, en *Lecciones de derecho penal parte especial*, V. II, Bogotá, Universidad Externado de Colombia, 2019.

SHERIDAN, Lorraine; GRANT, Tim. “Is cyberstalking different?”, en *Psychology Crime and Law*, No. 13 (6), Milton Park, Taylor & Francis, 2007.

SUÁREZ SÁNCHEZ, Alberto. *La estafa informática,* Bogotá, Ibáñez, UNAB, 2015.

SUÁREZ SÁNCHEZ, Alberto. *Manual de delito informático en Colombia*, Bogotá, Universidad Externado de Colombia, 2016.

THOMAS, Douglas; LOADER, Brian D. “Cybercrime: law enforcement, security and surveillance in the information age”, en THOMAS, Douglas; LOADER, Brian D. (eds.). *Cybercrime*, Routledge, New York, 2003.

VILLACAMPA ESTIARTE, Carolina. *Stalking y derecho penal,* Madrid, Iustel, 2009.

WESTRUP, Darrah; FREMOUW, William J. “Stalking behavior: A literature review and suggested functional analytic assessment technology”, en *Aggression and violent behavior*, No. 3:3, Elsevier, 1998.

YAR, Majid. *Cybercrime and society*, 2nd ed., London, SAGE, 2013.

YAR, Majid. “The novelty of cybercrime: An assessment in light of routine activity theory”, en *European Journal of Criminology*, No. 4 (2), Thousand Oaks, SAGE, European Society of Criminology, 2005.

Jurisprudencia

Corte Constitucional. Sentencia C-186 de 1996, M.P.: Vladimiro Naranjo Mesa.

Corte Constitucional. Sentencia T-478 de 2015, M.P.: Gloria Stella Ortiz Delgado.

Corte Suprema de Justicia, Sala de Casación Penal. Auto del 29 de marzo de 1989, M.P.: Jaime Giraldo Ángel.

Corte Suprema de Justicia, Sala de Casación Penal. Auto del 3 de agosto de 1989, M.P.: Jorge Carreño Luengas.

Corte Suprema de Justicia, Sala de Casación Penal. Sentencia SP107-2018, rad. 49799, M.P.: Fernando León Bolaños Palacios

Corte Suprema de Justicia, Sala de Casación Penal. Sentencia SP4573-2019, rad. No. 47234, M.P.: Eugenio Fernández Carlier.

Informes

PEÑA OCHOA, Paz (ed.). *Reporte de la situación de América Latina sobre la violencia de género ejercida por medios electrónicos*, Fundación Karisma *et ál*, noviembre de 2017. [https://karisma.org.co/descargar/latin-american-report-on-online-gender-violence/].

Reporteros Sin Fronteras. *Acoso en línea a periodistas: cuando los trolls arremeten contra la prensa*, 26 de julio de 2018. [https://rsf.org/es/noticias/rsf-publica-su-informe-acoso-en-linea-periodistas-cuando-los-trolls-arremeten-contra-la-prensa].

Notas de prensa

[https://www.bbc.com/mundo/noticias-46974250]

[https://www.elespectador.com/noticias/bogota/ejemplar-condenan-12-anos-de-carcel-acosador-en-transmilenio-articulo-839786]

[https://www.elespectador.com/noticias/bogota/caso-sergio-urrego-otro-fallo-historico-contra-la-discriminacion-articulo-829555]

[https://www.elespectador.com/opinion/editorial/la-endeble-defensa-de-mark-zuckerberg-articulo-890162.
https://www.france24.com/es/20190213-ligalol-periodistas-acoso-mujeres-internet]

[https://www.lasexta.com/noticias/sociedad/madre-suicida-madrid-difundirse-antiguo-video-sexual-suyo-trabajo_201905285ced13fb0cf21b72629c0631.html]

[https://www.portafolio.co/economia/empleo/el-acoso-laboral-crece-en-colombia-520447]

[https://www.telemundo51.com/noticias/destacados/Reto-Momo-crea-proecupacion-entre-los-padres--506468141.html]