UNIVERSIDAD DE CHILE
FACULTAD DE DERECHO
DEPARTAMENTO DE DERECHO PROCESAL

EMPLEO DE BOTS Y AGENTES ENCUBIERTOS PARA LA DETECCIÓN DEL CIBERACOSO Y SU VALOR PROBATORIO

-

Memoria para optar al grado de Licenciada en Ciencias Jurídicas y Sociales

MARÍA TERESA RODRÍGUEZ MANZANO

Profesora Guía: Lorena Donoso Abarca

Santiago, Chile

2021

A Gloria Rodríguez M. y Victoria López C.,
por ser el apoyo y sustento en los momentos más difíciles
de este largo proceso y en todos los momentos de mi vida.

Agradecimientos:

A mi familia.

A Victoria López Creo.

A Denisse Cornejo Matus.

A mi profesora, Lorena Donoso Abarca.

A la Universidad de Chile.

I.- ÍNDICE

II.- ÍNDICE DE TABLAS

III.- ACRÓNIMOS

COIP: Código Orgánico Integral Penal (Ecuador).

CONA: Código de la Niñez y Adolescencia (Ecuador).

DEA: Agencia Antidrogas de Estados Unidos.

INTECO: Institutito Nacional de Tecnologías de la Comunicación (España).

IP: *Internet Protocol address*.

NICHD: Instituto Nacional de la Salud infantil y Desarrollo Humano Eunice Kennedy Shriver (NICHD, por sus siglas en inglés)

NLU: *Natural Language Understanding*.

OAS: Organización de Estados Americanos.

SSI: Servicios de la sociedad de la información.

TIC: Tecnologías de la Información y la Comunicación.

IV.- RESUMEN

El desarrollo de las tecnologías de la información y comunicación (TIC) han significado un profundo cambio en la forma en que las personas se relacionan y se comunican entre sí, debido al surgimiento de nuevos canales de comunicación, como las llamadas 'redes sociales' y la gran cantidad de dispositivos electrónicos que permiten acceder a estas en cualquier momento y lugar. Sin embargo, esto no solo ha traído aparejado consecuencias positivas, sino que también negativas, como el surgimiento de nuevas formas de afectar los derechos de la persona. En particular nos interesa el ciberacoso, esto es, conductas agresivas o descalificadoras en contra de una persona, realizada a través de medios tecnológicos.

De acuerdo con diversos estudios, estas conductas tienen estrecha relación con problemas de carácter social y psicológico, tales como la baja autoestima, la depresión y la ansiedad. Cuando es un niño, niña o adolescente el afectado, además se relacionan con el ausentismo escolar, el bajo rendimiento académico y, en casos extremos, las autolesiones e incluso el suicidio.

Dada la gravedad de estas conductas, es que cobra relevancia la búsqueda de herramientas para la detección temprana del ciberacoso y otros fenómenos afines, tales como los discursos de odio, a fin de detectar y perseguir las responsabilidades de quienes hayan participado de estas conductas. En nuestra investigación analizamos la aplicabilidad de los '*bots*' en estas tareas.

Entendemos por '*bot*' un *software* o programa informático creado con la finalidad de realizar una tarea determinada para la que han sido programados. En este análisis el lector verá que cobra relevancia analizarlos conjuntamente con los denominados agentes encubiertos, pero además de manera individual, en cuanto a determinar el marco normativo que les es aplicable.

En nuestra investigación preliminar nos impusimos de la escasez normativa en nuestro entorno, tanto en materia sustantiva como procesal, sin embargo, encontramos experiencias en derecho comparado que podrían servir de ejemplo a seguir en el perfeccionamiento del marco jurídico nacional.

A estos aspectos nos referiremos en las páginas siguientes.

V.- INTRODUCCIÓN

En los últimos años, producto del desarrollo de la tecnología y, en especial, de la masificación de Internet como medio a través del cual se desarrollan interacciones humanas a distintas escalas, tanto a nivel de comunicaciones, como motores de búsqueda, medios de comunicación, redes sociales, y un largo listado de servicios que se han denominado "*servicios de la sociedad de la información*" (SSI), las personas han visto un cambio significativo en la manera de relacionarse entre sí. La creación de plataformas y medios habilitados para la comunicación les permite mantener o retomar el contacto con otras personas, tanto de círculos sociales cercanos, como entablar nuevas relaciones con gente de distintas partes del mundo, a partir de intereses comunes. Las redes sociales no solo traen desde el pasado a personas con las cuales se pudo tener interacción, sino que, además, sugieren "personas afines" a los intereses del sujeto, creando con ello una gran telaraña de contactos no solo a nivel ciudad, sino país e incluso planeta. Es así que se dice que las redes sociales "*son utilizadas tanto por individuos como por empresas, dado que permiten lograr una comunicación interactiva y dinámica*[1]". En efecto, la tecnología 'red social' no solamente se emplea en dicho ámbito, sino que, con el avance del tiempo, también se han extendido al ámbito corporativo, con la finalidad de expandir o dar a conocer un negocio, acercándolo a la población de interés de una forma sencilla y cómoda. Sin embargo, siempre existe un objetivo común: lograr una comunicación rápida y fluida entre las personas respecto de un tema de interés.

Además de las redes sociales, en lo que nos interesa, hemos asistido a una continua mejora de dispositivos electrónicos, los cuales permiten acceder a las redes sociales cada vez de una forma más sencilla. Hoy en día un teléfono celular es un dispositivo que permite un acceso a la web con muchas menos restricciones para sus usuarios, posibilitándoles la conexión prácticamente en cualquier momento y desde cualquier lugar en que se encuentren.

Desgraciadamente, esta mayor conectividad no solo ha implicado consecuencias positivas para la sociedad, sino que, producto de la masificación de los canales de comunicación vía

[1] HÜTT, H. (2012). *Las redes sociales: una nueva herramienta de difusión.* Reflexiones (Universidad de San José de Costa Rica),91(2): 121-128.

Internet, también ha traído aparejadas consecuencias negativas, a raíz de su mal uso por los usuarios, que han dado paso a distintos problemas en el ámbito social o incluso penal.

Dentro de estas malas prácticas podemos destacar los discursos de odio, y lo que más nos interesará analizar: el 'ciberacoso' o '*cyberbullying'*.

Bajo la expresión '*discurso de odio*' o '*hate speech*' se ha englobado a distintas acciones antijurídicas, o al menos contrarias a la ética y a la sana convivencia en una sociedad. Entre los ejemplos que se han mencionado como discursos de odio destacan la negación del holocausto, la promoción del exterminio de determinados grupos de personas tal como sucedió con el pueblo Tutsi, en Ruanda, la promoción de las conductas racistas, entre otras conductas que se caracterizan porque tienen como principal motor el odio hacia un grupo o tipo de personas o sector de la sociedad. Los efectos de estas conductas, además de atentar contra la dignidad humana y otras garantías fundamentales, tienen la capacidad de afectar gravemente la convivencia social.

Díaz Soto[2], citando a Waldron identifica "*cuatro formas que puede adoptar el discurso difamatorio contra una colectividad que, a su vez, lesiona la dignidad de sus miembros y, por tanto, debería estar proscrito por la ley; a saber:*

- La imputación de forma generalizada a los miembros de un grupo de la comisión de hechos ilícitos; como cuando se indica que todas las personas de color incurren en hurtos o violaciones.

- Mediante caracterizaciones que denigran a los miembros de la comunidad; como señalar que los judíos son avaros o maliciosos.

- A través de referencias a animales o cosas, de modo que se prive a los miembros de la colectividad atacada de su condición de seres humanos.

- Mediante prohibiciones en atención a los rasgos definidores del grupo, como prohibir la entrada a sitios públicos de personas de color".

[2] DÍAZ SOTO, José Manuel. "*Una aproximación al concepto de discurso del odio*" en Rev. Derecho Estado [online]. 2015, n.34, pp.77-101. ISSN 0122-9893. http://dx.doi.org/10.18601/01229893.n34.05, citando a Jeremy Waldron. The harm in hate speech, London, Harvard University Press, 2012 p.105-146 [Consulta: 15.09.2020].

De su parte, el 'ciberacoso', '*cyberbullyng*', 'acoso cibernético', 'acoso electrónico', 'acoso digital', o 'acoso por internet' se puede definir como "*aquella conducta agresiva e intencional mediada por dispositivos electrónicos, que se reitera en el tiempo y está dirigida por un individuo o grupo hacia una víctima que no puede defenderse por sí misma*[3]".

En adelante nos referiremos a este fenómeno simplemente como 'ciberacoso'.

El ciberacoso afecta múltiples aspectos en la vida de las personas que lo sufren, la salud mental, rendimiento escolar, desarrollo personal, son algunos de los ámbitos que podrían verse perjudicados por estas conductas.

En cuanto al impacto del ciberacoso, un estudio realizado por la Universidad Pontificia Bolivariana de Colombia en el año 2017[4], en que se entrevistó a 639 estudiantes de una media de 17,6 años revela que un 27,5% de la muestra había sido víctima de estas conductas. Entre los hallazgos, se deja a la luz la realidad de las consecuencias que padecen aquellas personas que han sido expuestas a situaciones de ciberacoso a través de las redes sociales, asociándose dicho fenómeno con varios problemas de salud mental, tales como el sentimiento de soledad, la depresión o la ansiedad. Asimismo, se revela que la violencia se da indirectamente, en formas tales como la intimidación, la discriminación, el hostigamiento o incluso la suplantación de identidad y la agresión a través de los medios digitales.

En Chile, de acuerdo con un artículo publicado por el Centro de Estudios MINEDUC, denominado "*Ciberacoso: una revisión internacional y nacional de estudios y programas*", de octubre de 2018, se señala que "*en nuestro país, un 8% de los padres tiene un hijo que ha experimentado ciberacoso, mientras que un 31% declara que un niño cercano a ellos lo ha sufrido*[5]".

[3] 13. REDONDO, J., et al (2017). *Impacto psicológico del ciberbullying en estudiantes universitarios: un estudio exploratorio*. Revista Colombiana de Ciencias Sociales, 8 (2): 458-478.
[4] Ibídem.
[5] Centro de Estudios MINEDUC. *Acoso: una revisión internacional y nacional de estudios y programas*. Santiago, Chile. 2018. [En línea] https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf. [consulta: 25.03.2021].

Por otro lado, y según los datos de la Superintendencia de Educación, "*las denuncias por ciberacoso han experimentado un alza del 64% de 2017 a 2018, esto es, de 104 denuncias en el periodo enero-julio de 2017 a 170 denuncias en el mismo semestre del año 2018*[6]".

Ante esta situación, se hace necesaria una solución que permita erradicar o mantener controlados estos fenómenos. Es aquí donde toman protagonismo los '*bots*', en relación con la figura de los 'agentes encubiertos' como mecanismos para rastrear en las redes, identificar a los responsables y detener los efectos nocivos de estas conductas.

Cuando hablamos de *bots* nos referimos a programas informáticos que pueden simular un comportamiento humano, realizando tareas repetitivas como el envío de mensajes o emails. Básicamente, un *bot* es un robot, pero sin un cuerpo físico o 'cuerpo robótico', cuyo plano de acción se encuentra dentro de Internet, pudiendo ser programado para localizar determinados patrones de comportamiento en la red. En el caso que nos ocupa, la detección de conductas que responden a las características de ciberacoso, realizadas a través de las redes sociales o en general, de Internet, para identificar a los agresores y obtener pruebas que permitan tomar las acciones legales pertinentes ante este tipo de conductas que afectan tanto a adultos como a jóvenes.

De su parte, los agentes encubiertos son funcionarios policiales cuya labor consiste en infiltrarse en una asociación u organización de carácter delictual, con el objeto de identificar a aquellas personas que tienen participación en los hechos y poder reunir antecedentes suficientes en el marco de una investigación.

Nos interesa determinar si las evidencias capturadas a través de estos medios, bajo la legislación chilena, podrían ser admitidas como prueba en juicio y, en caso de ser así, cómo se valorarían. Al respecto, nuestra legislación considera los agentes encubiertos en la Ley Nº 20.000 como "*el funcionario policial que oculta su identidad y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones con propósitos delictivos, con el objetivo de identificar a los partícipes, reunir información y recoger antecedentes*

[6] GUEVARA, Javier; STHIOUL, Alberto; RIVERA, Mario; BARRIENTOS, Fernando. *Ciberacoso: una revisión internacional y nacional de estudios y programas*. Centro de Estudios Mineduc. Evidencias Nº 43. noviembre 2018. [En línea] en https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf. [consulta: 06.07.2020].

necesarios para la investigación[7]". Luego, el Código Procesal Penal regula los aspectos relativos a su intervención en los procedimientos en los artículos 366 y siguientes del Código Procesal Penal. Sin embargo, esta normativa parte de la base de un sujeto humano, que es quien realiza estas labores. De nuestra parte nos interesa desvelar si se pudiese reconocer estos efectos jurídicos cuando se realiza la labor propia de los 'agentes' a través de *bots*.

Para abordar estos temas, en primer lugar, revisaremos los conceptos de los principales fenómenos que se producen por el uso indebido de Internet, como los discursos de odio y, más en profundidad, el ciberacoso, con especial mención a aquellos casos en que estas conductas son realizadas a través de medios tecnológicos, así como el surgimiento de este, sus efectos y su regulación en la legislación chilena y en el derecho comparado.

A continuación, se describirán los conceptos de '*bot*' y 'agente encubierto', y se analizará el marco jurídico de los agentes encubiertos en Chile y derecho comparado, para los efectos de analizar si nuestro marco jurídico requiere actualizaciones que permitan su admisibilidad, en caso de considerarse útiles en el marco de estas investigaciones, al menos.

Un aspecto que debemos considerar en la determinación de la legalidad de estas medidas dice relación con la edad de los participantes, puesto que, al tratarse de una medida intrusiva, deberán establecerse especiales resguardos en aquellos casos que los sujetos involucrados sean niños, niñas o adolescentes, más aún si se trata de impúberes. A este respecto cobrará relevancia el análisis de los derechos de estos sujetos, en su configuración a partir del interés superior del niño y la autonomía progresiva de los menores como justificación en la aplicación de medidas intrusivas para la detección del ciberacoso en etapa escolar.

Para este caso, la regulación relevante serán fundamentalmente las normas de la Constitución Política de la República, las normas del Código Penal -en lo referente a los mensajes que constituyen amenazas, acoso u otros delitos mediante las redes sociales-, así como

[7] ZAVIDICH, Carolina. *El Agente Encubierto y su responsabilidad*. Unidad Especializada de Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas. [En línea] en http://www.fiscaliadechile.cl/observatoriodrogaschile/documentos/publicaciones/articulo_25_ley_20000_agente_encubierto_CZ.pdf [consulta: 06.04.2021].

los tratados internacionales y ciertas y determinadas normas de derecho comparado que podrían ser adoptadas en Chile a futuro.

Si bien nuestro trabajo tiene como objetivo hacer un análisis del fenómeno del ciberacoso, así como de las iniciativas de prevención de este a nivel nacional, para poder determinar qué acciones han sido practicadas en Chile para afrontar esta nueva modalidad de acoso, y qué tan viables podría ser la implementación de *bots* o agentes encubiertos con la tecnología y legislación actual, qué derechos podrían verse eventualmente afectados con la aplicación de estas medidas intrusivas y cuál sería el valor probatorio de estas medidas, estimamos que estos análisis podrían ser empleados en la definición del uso de estas tecnologías en la pesquisa de otros fenómenos delictivos.

En cuanto al **objetivo general** de nuestra investigación, lo hemos circunscrito a analizar la factibilidad de la implementación de *'bots*' o '*agentes encubiertos electrónicos'* como medio para pesquisar y acreditar en juicio las conductas asociadas a discursos de odio y ciberacoso que se realizan a través de Internet.

Para ello determinamos los siguientes **objetivos específicos**, que a su vez hemos 'problematizado' para los efectos de dar un curso lógico a la exposición de resultados:

En primer lugar, nos hemos fijado como objetivo responder a la pregunta ¿En qué consisten las conductas de ciberacoso y los discursos de odio en Internet? ¿cómo han sido recogidos en el ámbito normativo, doctrinario y jurisprudencial?

En el ámbito técnico, nos hemos centrado en los *'bots'* a efectos de describir su funcionamiento y analizar sus posibles semejanzas con los agentes encubiertos, especialmente en la detección y análisis de antecedentes o fenómenos que suceden en la Red.

En tercer lugar, hemos analizado la doctrina y normativa relativa a los agentes encubiertos y su posible aplicación a los *bots* en derecho comparado y en Chile. En este aspecto, nos hemos centrado en conflictos jurídicos que se ventilan a raíz de la potencial implementación de *bots* y agentes encubiertos para la detección del ciberacoso, especialmente en relación a los niños niñas y adolescentes.

Ya en el ámbito procesal, nos hemos preguntado por las posibilidades de aportar en el proceso los resultados de las investigaciones realizadas a través de *bots* y su eventual valor probatorio.

Finalmente, atendido que intuimos que nuestro derecho no estaba preparado para estos fenómenos y luego lo confirmamos, nos centramos en las posibles modificaciones que requeriría nuestra legislación para admitir estos medios de prueba. Al respecto, nos hemos referido al encuadre de estos medios en los esquemas probatorios en Chile, especialmente en lo que dice relación con su aportación probatoria y valoración por el tribunal.

Para cumplir con estos objetivos hemos analizado la normativa nacional, así como los tratados internacionales y diversas normativas de derecho comparado.

En cuanto a los aspectos metodológicos, nos hemos basado en el método dogmático jurídico. Se partirá por lo más general, describiendo el fenómeno tecnológico, su origen y efectos, para posteriormente precisar respecto de su actual regulación en la normativa chilena e internacional y, finalmente, analizar su aplicación probatoria.

CAPÍTULO I. EL CIBERACOSO EN INTERNET

Distintas formas de odio a través de Internet han llamado la atención a nivel internacional. En el seno de las Naciones Unidas, incluso, se ha elaborado "*La estrategia y plan de acción de las Naciones Unidas para la lucha contra el discurso de odio*[8]", en atención a que advierten el riesgo de la proliferación de la intolerancia, la discriminación, la hostilidad y violencia en las sociedades que lo sufren. En este documento se define discurso de odio en los siguientes términos "*cualquier forma de comunicación de palabra, por escrito o a través del comportamiento, que sea un ataque utilice lenguaje peyorativo o discriminatorio en relación con una persona o un grupo sobre la base de quiénes son o, en otras palabras, en razón de su religión, origen étnico, nacionalidad, raza color, ascendencia, genero u otro factor de identidad*". En todo caso, lo que se proscribe no es el discurso de odio en sí, sino la 'incitación', esto es, la utilización de la expresión con el objeto explícito y deliberado de dar lugar a discriminación, la hostilidad o la violencia.

En lo que nos interesa, el documento se refiere al uso de la tecnología y su relación con este fenómeno, en los siguientes términos: "*las entidades de las Naciones Unidas deben adaptarse a las innovaciones tecnológicas y alentar la realización de más investigaciones sobre la relación entre el uso indebido de internet y las redes sociales para difundir el discurso de odio y sobre los factores que impulsan personas a cometer actos de violencia. Las entidades de las Naciones Unidas también deben colaborar con agentes del sector privado, incluidas las empresas de medios sociales, en relación con las medidas que puedan adoptar para apoyar los principios de las Naciones Unidas para afrontar y contrarrestar el discurso de odio, fomentando las alianzas entre los gobiernos, la industria y la sociedad civil*."

La Unesco también ha propuesto una definición de 'discurso de odio', en los siguientes términos: "*expresiones a favor de la incitación a hacer daño (particularmente a la discriminación, hostilidad o violencia) con base en la identificación de la víctima como perteneciente a determinado grupo social o demográfico. Puede incluir, entre otros, discursos*

[8] ONU. "*La estrategia y plan de acción de las naciones unidas para la lucha contra el discurso de odio".* [En línea] en https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_ES.pdf [consulta: 06.04.2021].

que incitan, amenazan o motivan a cometer actos de violencia. No obstante, para algunos el concepto se extiende también a las expresiones que alimentan un ambiente de prejuicio e intolerancia en el entendido de que tal ambiente puede incentivar la discriminación, hostilidad y ataques violentos dirigidos a ciertas personas[9]".

Asimismo, la Organización de Estados Americanos (OAS) ha puesto sus ojos sobre los discursos de odio y la incitación a la violencia contra las personas lesbianas, gays, bisexuales, trans e intersex en América. Esto, por cuanto estas acciones se han traducido en afectaciones concretas contra la vida, integridad física y psíquica de las personas LGBTI.

En el seno de la Unión Europea, se ha entendido por discurso de odio, aquel que se encamina al "f*omento, promoción o instigación (...) del odio, la humillación o el menosprecio de una persona o grupo de personas, así como el acoso, descrédito, difusión de estereotipos negativos, estigmatización o amenaza con respecto a dicha persona o grupo de personas y la justificación de esas manifestaciones por razones de 'raza', color, ascendencia, origen nacional o étnico, edad, discapacidad, lengua, religión o creencias, sexo, género, identidad de género, orientación sexual y otras características o condición personales*[10]".

En nuestro entorno, "*bajo el sistema interamericano de protección de derechos humanos los Estados sólo están obligados a prohibir el discurso de odio en circunstancias limitadas, esto es, cuando el discurso constituya incitación a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por motivos que incluyen la raza, el color, la religión, el idioma o el origen nacional, entre otros (Artículo 13.5 de la Convención Americana)*[11]".

De nuestra parte, en nuestra investigación nos centraremos en el "*bullying*", como fenómeno y nos referiremos a la aplicación de los *bots* como medio de pesquisa y eventualmente

---

[9] UNESCO. *Combatiendo el Discurso de Odio en Línea* [Countering Online Hate Speech], https://unesdoc.unesco.org/ark:/48223/pf0000233231_eng. 2015, págs. 10 -11. [consulta: 06.04.2021]

[10] Recomendación nº 15 de la Comisión Europea contra el Racismo y la Intolerancia (ECRI) del Consejo de Europa. 2015.

[11] OAS. Relatoría sobre los Derechos de las personas Lesbianas, Gays, Bisexuales, Trans e Intersex y la Relatoría Especial para la Libertad de Expresión de la CIDH. Capítulo IV. Discurso de Odio y la Incitación a la violencia contra las personas lesbianas, gays, bisexuales, trans e intersex en América. [En línea] Aprobado por la Comisión Interamericana de Derechos Humanos el 12 de noviembre de 2015. http://www.oas.org/es/cidh/expresion/docs/informes/odio/Discurso_de_odio_incitacion_violencia_LGTBI.pdf [consulta: 06.04.2021].

como prueba en juicio de estas conductas. Si bien el '*bullying'* es un fenómeno que siempre ha estado presente entre los jóvenes, no siendo un problema exclusivo de la época actual, hoy en día, debido a la masificación de servicios de comunicaciones e información que funcionan sobre la Red Internet, tales como sistemas de mensajería y de las redes sociales, se ha extendido preocupantemente la realización de esta conducta, no solo en niños, sino que también tratándose de adultos, que son víctimas de ciberacoso, discursos de odio y amenazas a través de la red.

En los últimos años se han difundido mediante los medios de comunicación la existencia de casos graves, que han puesto de manifiesto la importancia de tomar medidas respecto del tema, puesto que dicho problema puede tener serias consecuencias en las víctimas que lo sufren, sobre todo en los niños intimidados, que incluso pueden llegar a situaciones tan extremas como el suicidio.

El ciberacoso, por tanto, se produce junto con las formas tradicionales de acoso, por lo que se define desde el mismo marco que este, entendiéndose como "*la intimidación o agresión intencional y continua, infligida a través de medios electrónicos como computadores, teléfonos móviles, internet u otros dispositivos electrónicos, y que implica un desbalance de poder entre quien agrede y la víctima*[12]".

El ciberacoso consiste en el envío o publicación de contenido ofensivo o falso respecto de otra persona, con el objeto de causar en esta un sentimiento de humillación, ira o miedo frente a la misma persona o al grupo al cual pertenece.

Lo que ha alertado a nivel internacional respecto de este fenómeno en relación con el acoso tradicional es el impacto que puede llegar a tener en la persona, por cuanto la agresión se puede ver potenciada por el medio que se emplea, que además de la mayor audiencia a la que puede llegar, se une al potencial anonimato del agresor y al hecho de que no reconoce limitaciones de tiempo y espacio, sino que puede ser provocado en cualquier momento y lugar.

[12] GUEVARA, Javier; STHIOUL, Alberto; RIVERA, Mario; BARRIENTOS, Fernando. *Ciberacoso: una revisión internacional y nacional de estudios y programas*. Centro de Estudios Mineduc. Evidencias Nº 43, p. 4. Noviembre 2018. [En línea] en https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf [consulta: 06.07.2020].

En el último tiempo, y de manera diaria, una gran cantidad de jóvenes se han visto involucrados en situaciones de ciberacoso, siendo tanto autores de este como víctimas. Entre los medios que se utilizan destacan las redes sociales y sistemas de mensajería a través de Internet, o aplicaciones, por lo que se vuelve más intenso. Como efectos preocupantes en los jóvenes, el ciberacoso impacta en el rendimiento académico, en el comportamiento, en la salud mental tanto del afectado como del grupo en el cual se produce, pudiendo incluso llegar a impactar en la salud física o la vida de la persona.

Los tipos de ciberacoso escolar -al igual que en el acoso tradicional- son múltiples y variados, siendo el más común aquel que es efectuado mediante burlas, amenazas o insultos, entre otros, pero también puede tener como intención excluir a alguien de algún grupo o causar un daño en su imagen pública frente a sus pares mediante la difusión o invención de rumores que puedan provocar gran vergüenza en el afectado.

Un primer paso para lograr hacer frente a este fenómeno es tomar conocimiento de que los niños están siendo víctimas de ciberacoso, o sometiendo a este a sus pares. Si bien una herramienta para ello es el diálogo, en muchas ocasiones esto no es efectivo o posible, debido a la vergüenza o temor que el niño, niña o adolescente afectado, pueda sentir al considerar la idea de comunicar que está siendo víctima de ciberacoso, por lo que es necesario contar con un mecanismo distinto para poder detectar lo que estos jóvenes viven de manera oportuna, antes que se produzcan efectos graves en su salud mental o física. Asimismo, en aquellos casos que se produzcan hechos graves, que puedan revestir caracteres de delito o en aquellos en que los menores incurran en autolesiones graves, y sea necesario intervenir o investigar, podría resultar útil la implementación de los ya mencionados *bots*, los cuales podrían programarse para la detección de ciertas palabras y conceptos que los ayudase a dilucidar cuándo estamos frente a un discurso de odio, amenazas o ciberacoso.

La medida señalada se hace necesaria, en síntesis, para la tranquilidad y seguridad tanto de personas adultas como, sobre todo, los niños en etapa escolar.

Estimamos que, mediante la implementación de mecanismos como los *bots* que pudieran ayudar a detectar, sancionar y erradicar los discursos de odio y las conductas de ciberacoso,

estos podrían disminuir notablemente, reportando así un mayor beneficio a la sociedad, y asegurándose de manera más eficaz el respeto a la dignidad e igualdad de las personas.

1.- Concepto de ciberacoso

El término '*ciberacoso*', también conocido como '*ciberbullying*', se ha hecho presente cada vez con más frecuencia en los últimos años en los medios de comunicación y en conversaciones en entornos sociales más cerrados, fundamentalmente a través de la televisión e Internet, pero también en reuniones escolares entre padres y profesores de centros educacionales y en reuniones familiares en las cuales alguno de los integrantes, especialmente jóvenes, lo sufren día a día. Esta frecuencia en el tratamiento del tema no es casual, sino que da cuenta de una realidad: el acoso que afecta a miles de personas alrededor del mundo entero, especialmente a niños y adolescentes.

Como señalamos antes, el 'ciberacoso', '*cyberbullyng*', 'acoso cibernético', 'acoso electrónico', 'acoso digital', o 'acoso por internet' se puede definir como "*aquella conducta agresiva e intencional mediada por dispositivos electrónicos, que se reitera en el tiempo y está dirigida por un individuo o grupo hacia una víctima que no puede defenderse por sí misma*".[13] También se ha definido como "*cualquier comportamiento realizado a través de medios electrónicos o digitales por individuos o grupos que comuniquen repetidamente mensajes hostiles o agresivos destinados a infligir daño o incomodidad a otros*[14]".

Si bien en la segunda definición citada se omiten las cualidades de la víctima, mantiene el componente tecnológico, la naturaleza hostil del acto, la intención de infligir un sufrimiento a la víctima y la repetitividad. Sin embargo, debemos tener presente que, por la naturaleza del medio, bastará con que el primer agresor lance una vez el mensaje a la red, para que terceros se

[13] REDONDO, J., LUZARDO-BRICEÑO, M., GARCÍA-LIZARAZO, K. L. e inglés, C. J. *Impacto psicológico del ciberbullying en estudiantes universitarios: un estudio exploratorio*. Revista Colombiana de Ciencias Sociales, 8 (2), pp. 458-478. 2017.

[14] BARBOZA G. (2018). *The association between school exclusion, delinquency and subtypes of cyber- and F2F-victimizations: identifying and predicting risk profiles and subtypes using latent class analysis*. Child Abuse Negl. Citado por TORRES-MONTILLA, Y., en "Características del ciberacoso y psicopatología de la víctima". Repertorio de Medicina y Cirugía 27(3):189-196].

ocupen de amplificarlo, por lo que la repetitividad no pareciera ser un elemento esencial del concepto.

Adicionalmente, de esta definición extraemos que en el ciberacoso **se emplean los medios digitales**, tales como teléfonos celulares, redes sociales y, en general, Internet, **para efectuar conductas dañinas** hacia terceros, con la **intención de acosarlos psicológicamente**.

En términos generales, el acoso suele darse entre iguales, por lo que es frecuente que agresor y víctima compartan un contexto social.

El Observatorio INTECO de España, dedicado a estudiar la relación de las personas con las tecnologías de la información y la comunicación, define el ciberacoso como: "*acoso entre iguales en el entorno TIC, e incluye actuaciones de chantaje, vejaciones e insultos de niños a otros niños*[15]".

Sin embargo, el ciberacoso no es una conducta que solo se produce entre los niños, ya que existe cada vez con mayor frecuencia la práctica de personas mayores de edad que recurren a estos medios con la finalidad de agredir verbalmente a terceros -fundamentalmente exparejas o incluso figuras públicas o personas de reputación connotada- y, en ocasiones, configurar delitos de acoso y/o amenazas, entre otros.

2.- Origen del fenómeno del ciberacoso

El ciberacoso surge de manera coetánea a la masificación de los dispositivos tecnológicos personales, que precisamente permiten el acceso a Internet y, por tanto, a las redes sociales.

Respecto a los factores asociados con el ciberacoso y su prevalencia, se han realizado estudios para detectar correlaciones entre estas conductas y diversas variables de interés, como las características que poseen tanto los agresores como las víctimas, sus familias y entornos.

[15] INTECO. *Estudio sobre hábitos seguros en el uso de las TIC por los menores*. 2009. [En línea] https://faros.hsjdbcn.org/es/noticia/estudio-sobre-habitos-seguros-uso-tic-ninos-adolescentes-confianza-padres. [consulta: 06.04.2021].

En nuestro país, a vía ejemplar, el Centro de Estudios del Ministerio de Educación de Chile[16], analizando los resultados de investigaciones internacionales, releva que en la vereda de la perpetración del ciberacoso destacan como principales predictores de la perpetración de conductas de ciberacoso: "*el uso riesgoso de tecnologías de la información y las comunicaciones, la desconexión moral, la depresión, las normas sociales y el acoso tradicional son los principales predictores de la perpetración del ciberacoso"… "las creencias normativas sobre la agresión"* (pág. 5)

En contraste, respecto de las víctimas serían factores prevalentes *"el uso riesgoso de TIC y la victimización del acoso tradicional*", a lo que suman las ideas suicidas y la depresión.

Ligado al ciberacoso, el estudio revela que asociado a estas conductas se revelan uso de sustancias tales como drogas, alcohol y tabaco.

En México, el estudio "*Variables que discriminan el perfil del ciberacosador en adolescentes mexicanos*[17]". destaca, en lo que nos interesa, que en el ciberacoso el potencial anonimato del agresor, las posibilidades de simular identidades diferentes, el medio que favorece la desinhibición de la persona y el empoderamiento digital de los nativos digitales alimenta los climas de toxicidad y círculos de interacción nociva entre personas o grupos. A ello se suma "*la escasa interacción relacional entre los participantes, situación virtual que provoca la falta de empatía del agresor con la víctima y la conciencia de daño provocado; a su vez, la amplia audiencia potencia las agresiones en lo privado y en lo público llegando a un gran número de espectadores sin controlar la situación y produce efectos devastadores en la víctima*[18]".

[16] GUEVARA, Javier; STHIOUL, Alberto; RIVERA, Mario; BARRIENTOS, Fernando. *Ciberacoso: una revisión internacional y nacional de estudios y programas*. Centro de Estudios Mineduc. Evidencias Nº 43, noviembre 2018. [En línea] en https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf [consulta: 06.07.2020].

[17] CASTRO, C. et al (2019). Revista de Psicología y Ciencias del Comportamiento de la Unidad Académica de Ciencias Jurídicas y Sociales. 10(2): 30-43.

[18] Ibídem p. 31.

3.- Características del ciberacoso

Como ya anticipáramos, el ciberacoso, debido a los medios que son empleados para la realización de esta conducta de hostigamiento hacia la víctima, reviste un carácter de mayor gravedad, puesto que el agresor utiliza ciertas ventajas de la red en su beneficio para verse protegido de las posibles consecuencias, tales como:

1) **El anonimato**, toda vez que Internet otorga una suerte de 'ventaja estratégica' del acosador por sobre su víctima, y una mayor indefensión de estas últimas respecto a su acosador. En muchas ocasiones, el acosador realiza esta conducta mediante perfiles falsos o, directamente, a través de redes que permiten el envío de mensajes sin identificación previa, tales como '*ThisCrush*' o '*F3*', plataformas surgidas en los últimos años y populares entre los adolescentes, en las cuales sus usuarios pueden publicar mensajes o preguntas anónimas, y que se han visto empleadas para conductas de acoso, humillaciones o perpetración de amenazas e incluso injurias o calumnias contra el usuario.

2) **La falta de percepción real del daño**, lo cual provoca que el ciberacoso sea una modalidad de acoso mucho más agresiva y violenta psicológicamente, puesto que el agresor, al no ver personalmente a su víctima a través de Internet, presenta una menor empatía por el daño causado mediante sus actos. En ocasiones, no siendo siquiera consciente de la gravedad de sus acciones.

3) **El alcance de personas al que pueden llegar las publicaciones efectuadas en Internet**, puesto que en muchas ocasiones, el ciberacoso no solo se presenta a través de mensajes vía privada a la víctima, sino que también se presenta en forma de publicaciones abiertas ante una determinada comunidad que forma parte de la plataforma -o para quienes la visitan recurrentemente- en que son expuestas declaraciones que impliquen un menoscabo en la persona a la cual van dirigidas, tales como humillaciones y, en casos extremos, la atribución de hechos que pueden llegar a revestir el carácter penal de la injuria y la calumnia, situación que ocurre en las llamadas 'funas', en que una persona, supuestamente víctima de una actitud reprochable por parte de la persona que está siendo 'funada', denuncia públicamente los hechos sufridos a manos de esta, con el objeto de advertir a la comunidad sobre la peligrosidad del sujeto en cuestión, con la finalidad de que el resto pueda estar al tanto de los actos repudiables

de tal persona y evitar ser víctima de los mismos; pero que, sin embargo, en muchas circunstancias son usadas también maliciosamente para dar testimonios falsos sobre alguien cuya imagen se pretende menoscabar frente a un amplio grupo de personas por motivos de índole personal, llegando tanto a conocidos como desconocidos de esa persona, provocándole daños de carácter moral, tales como ansiedad y problemas de autoestima.

4.- Paralelo entre el acoso tradicional y el ciberacoso

A pesar de la atención que ha recibido el fenómeno del ciberacoso, tanto en los medios de comunicación, como en la comunidad académica y en el ámbito familiar, entre otros, aún sigue abierta la discusión sobre si es posible tratarlo de la misma manera que el acoso tradicional, atendido que, como señalamos, en el ciberacoso no resulta tan evidente establecer el criterio de repetición, propio del acoso tradicional. Asimismo, no sería un requisito el desequilibrio de poder entre el acosador y la víctima. Sin perjuicio de lo anterior, si entendemos por ciberacoso "*la intimidación o agresión intencional y continua, infligida a través de medios electrónicos como computadores, teléfonos móviles, internet y otros dispositivos electrónicos, resultando un desbalance de poder entre el agresor y la víctima*[19]", podremos apreciar que ambas conductas comparten más de una característica.

En efecto, tanto el ciberacoso como el acoso tradicional tienden a producir efectos negativos similares en las personas que son víctimas de él en cualquiera de sus modalidades. Sin embargo, dadas las características a que nos referimos antes, el ciberacoso provoca un mayor impacto en la víctima, ya sea por la amplificación de la agresión como la persistencia en el tiempo y las dificultades asociadas a la eliminación de los mensajes, en un medio que ha sido diseñado para que la información se mantenga disponible en el tiempo. Esto es especialmente grave para los más jóvenes y aquellos que sufren ciertas circunstancias que puedan hacerlos aún más vulnerables, tales como personas aquejadas por algún problema familiar o que estén atravesando momentos difíciles emocionalmente.

[19] GUEVARA, Javier; STHIOUL, Alberto; RIVERA, Mario; BARRIENTOS, Fernando. *Ciberacoso: una revisión internacional y nacional de estudios y programas*. Centro de Estudios Mineduc. Evidencias Nº 43, p. 6. Noviembre 2018. [En línea] en https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf [consulta: 06.07.2020].

Mientras en el acoso tradicional se incluyen conductas tales como insultos continuos, apodos denigrantes, golpes o amenazas de maltrato físico, y la invención de falsos rumores sobre la persona acosada en su círculo social habitual, dentro de conductas propias del ciberacoso se incluye el envío y publicación de contenido ofensivo o falso sobre aquella persona a la cual se dirige esta conducta, causándole sentimientos tales como humillación, vergüenza, temor, etc.

"*En los estudios de investigación financiados por el NICHD también se encontró que, a diferencia de lo que ocurre con las formas tradicionales de intimidación, los jóvenes que son víctimas de intimidación cibernética —por ejemplo a través de la computadora o el celular— tienen un riesgo mayor de sufrir depresión que los jóvenes que realizan la intimidación*[20]". De ahí que tanto las familias como las comunidades educativas deban adoptar medidas efectivas contra este fenómeno.

El trabajo contra el ciberacoso es transversal; involucra a las instituciones relacionadas a educación, justicia, salud y desarrollo social, lo cual da cuenta del impacto y trascendencia de la lucha contra este flagelo.

La víctima podrá verse afectada en el ámbito académico, en su salud y la de su familia. Incluso hay preocupación por las secuelas que el ciberacoso puede llegar a provocar de forma severa (depresión, ansiedad, baja autoestima), como también, finalmente, en el ámbito judicial hay un interés en generar una regulación a este fenómeno mediante la tipificación o adaptación de diversos delitos que cada vez con mayor frecuencia son perpetrados por medios digitales, como las amenazas, las injurias o las calumnias.

[20] KENNEDY SHRIVER, Eunice. *National Institute of Child Health and Human Development. "Focus on children's mental health research at the NICHD*". 2012. [En línea] en https://www.nichd.nih.gov/newsroom/resources/spotlight/060112-childrens-mental-health [consulta: 09.07.2020]

A continuación, a modo de resumen, se muestra una tabla comparativa[21] entre las características del acoso tradicional o "bullying" y el ciberacoso o "ciberbullying":

BULLYING	CIBERBULLYING
Cara a cara	Anónimo
Es un grupo o individual	Individualmente
Golpes, empujones, agresión verbal o exclusión social	Mensajes, e-mail, imágenes manipuladas
Solo en horas de escuela	En todos lados y a toda hora
Se limita a la agresión directa	Sin límite de alcance
Solo audiencia escolar	Audiencia ampliada por Internet
Certeza de que solo se encuentra en el ámbito escolar	Incertidumbre de no saber quién ha visto las imágenes o mensajes
Víctima y agresor; víctima-agresor	Cibervíctima-Ciberagresor
Posibilidad de que caiga en el olvido	Persistencia de la información publicadas en las redes y sistemas de información

Tabla 1

5.- Efectos del ciberacoso

Como señalamos antes, el ciberacoso afecta múltiples aspectos en la vida de las personas que lo sufren. En las personas adultas, si bien el fenómeno puede tener un impacto menor, debido a la madurez emocional de la víctima, también hay susceptibilidad a padecer trastornos

[21] JOFFRE, V. M. et al (2011). *Bullying en alumnos de secundaria, características generales y factores asociados de riesgo*. Boletín Médico del Hospital Infantil de México 68(3): 193-202.

psicológicos producto de haber sido víctimas de estas conductas, dependiendo de la gravedad de los hechos, puesto que, si bien pueden ser indiferentes a comentarios que pretenden ridiculizarlo mediante descalificativos, pueden existir otras conductas que los hagan sentirse inseguros y vulnerables por afectar un ámbito más íntimo de la persona.

Un ejemplo comúnmente visto es el caso de exparejas que pretenden acosar, extorsionar o amenazar vía redes sociales a una persona con la cual alguna vez mantuvieron una relación, presionándola a realizar una conducta determinada bajo amenaza de que, en caso contrario, secretos o fotos íntimas de esta persona serán publicadas en la red, que se ha estimado que configuraría el delito de 'amenazas condicionales' del artículo 296 Nº 1 del Código Penal.

En otros casos, directamente la víctima se encuentra en la situación de que estas fotos íntimas fueron compartidas en Internet sin su consentimiento, llegando a ojos de un amplio público, habiendo un atentado a su derecho a la privacidad, lo cual produce vergüenza y un evidente menoscabo en la salud mental de la víctima. Estas conductas han sido recogidas en la normativa de diversos países bajo la denominación de '*revenge porn'*. Así lo ha analizado Cavada[22] (2018), quien en su análisis determina que "*en las legislaciones de Alemania, Brasil, Canadá, España, Estados Unidos de América, Reino Unido y Nueva Zelanda se han encontrado normas que sancionan directamente el llamado revenge porn, o la difusión de imágenes íntimas sin autorización del afectado o contra su voluntad. Así mismo, en Perú y Puerto Rico se han encontrado normas que podrían sancionar esta conducta, dependiendo de la interpretación que se dé al texto legal*." Si bien no todas las normas a que alude son de índole penal, sino que habrá sanciones civiles y administrativas en algunos casos. En el caso de Chile, podrían aplicarse a esta materia las figuras del artículo 438 del Código Penal (extorsión), la del artículo 161-B de este mismo cuerpo normativo (amenazas) o la figura del artículo 296 y ss. del Código Penal (amenazas condicionales), esto dependiendo de las circunstancias de cada caso.

Este mismo autor señala como relevante en estos casos, que "*La Ley N° 19.423, de 1995, introdujo dos nuevos artículos, ya señalados, en el párrafo quinto 'De los delitos contra el respeto y protección a la vida privada y pública de la persona y su familia' del Código Penal:*

[22] CAVADA H. Juan Pablo, "*Revenge Porn. Legislación extranjera*". Biblioteca del Congreso Nacional de Chile. Asesoría Técnica Parlamentaria. Diciembre, 2018, Nº SUP 118573 [consulta: 10.05.2021]

el artículo 161-A que sanciona diversos atentados en contra de la intimidad, que en términos generales se refieren a la captación y difusión de información privada en los términos que en esa disposición se indica, y el artículo 161-B que, vinculado a la norma anterior, contiene una figura especial de chantaje. Dicho artículo 161-A contempla distintos tipos penales que protegen la intrusión en la vida íntima, la indiscreción o deslealtad en las comunicaciones y las actuaciones privadas, y la difusión de información obtenida mediante una intromisión o indiscreción", haciendo presente que ninguno de estos tipos incluye la difusión de imágenes que han sido capturadas con la autorización del afectado, y luego difundidas con o sin su consentimiento.

A pesar de esto, debido a que en gran parte de los casos de ciberacoso entre personas adultas suelen cometerse delitos con una tipificación específica para cada tipo de acto realizado, la mayor preocupación está enfocada en el ciberacoso entre los niños y adolescentes, donde no necesariamente siempre existe una figura delictual y en que la víctima posee una mayor vulnerabilidad ante estos ataques. A lo anterior se suma el que sufrir ciberacoso aumenta la probabilidad de tener problemas relacionados a comportamiento y rendimiento académico, especialmente si se dan simultáneamente otros problemas como el abuso por parte de los profesores, abandono de los padres, disfunción familiar o el desarrollo en un entorno de pobreza, entre otros.

En este ámbito, un estudio de Kowalski y Limber, en el año 2013, analizó la relación entre las experiencias de niños y adolescentes con ciberacoso y acoso tradicional, así como la salud psicológica y física y el rendimiento académico de estos. Mediante la aplicación de encuestas anónimas a estudiantes de Pennsylvania se determinó que "*participantes en los grupos de acosadores / víctimas (y particularmente el grupo de ciberacoso / víctima) tuvieron los más altos puntajes negativos en la mayoría de las medidas de salud psicológica y física y rendimiento académico. Esto sugiere que parece haber una superposición sustancial, aunque no perfecta, entre la participación en acoso tradicional y ciberacoso. Además, las correlaciones físicas, psicológicas y académicas de los dos tipos de acoso se parecían entre sí*[23]".

[23]GUEVARA, Javier; STHIOUL, Alberto; RIVERA, Mario; BARRIENTOS, Fernando. *Ciberacoso: una revisión internacional y nacional de estudios y programas*. Centro de Estudios Mineduc. Evidencias Nº 43, p. 6. Noviembre 2018. [En

6.- El ciberacoso en niños en edad escolar

La preocupación por el crecimiento del fenómeno del ciberacoso otorga una especial importancia a su detección en los niños en edad escolar que lo sufren por parte de sus pares desde edades tempranas, en consideración a que "*Aquellos que son víctimas de intimidación tienen mayor riesgo de desarrollar problemas de salud mental, dolores de cabeza y problemas de adaptación en la escuela*[24]". Esto se debe a que se encuentran en una etapa esencial de la vida, en la cual comienzan a forjar su personalidad y su percepción sobre ellos mismos, lo que los hace especialmente vulnerables a estos ataques, pudiendo la intimidación afectar su salud física y emocional, ya sea a corto plazo como a lo largo de sus vidas, llegando incluso a ocasionar lesiones físicas, problemas sociales o problemas emocionales.

i.- Formas y efectos del ciberacoso en los niños

Conociendo las características que reviste el ciberacoso y su efecto en la población general, es necesario poner especial énfasis en cómo este afecta a los niños más pequeños.

Si bien los nuevos dispositivos tecnológicos solucionan la vida en muchos sentidos, es necesario controlar el acceso que poseen los más pequeños a estos para evitar los casos de acoso cibernético. En este caso, si bien el ciberacoso comparte conductas en común con aquel que puedan sufrir adultos o adolescentes, durante la etapa de edad escolar más temprana suele manifestarse en ataques de las siguientes formas:

a) El robo de identidad en redes sociales, mediante el cual los niños crean perfiles falsos con el objeto de divulgar secretos del que está siendo víctima del ataque, o agredir a conocidos de dicha víctima para deteriorar sus relaciones sociales.

b) El chantaje, a través del cual el acosador posee datos o inventa rumores comprometedores sobre la víctima, con los que posteriormente lo extorsiona para lograr que este actúe a su voluntad si no quiere que dicha información sea revelada. Por lo general, los

línea] en https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf [consulta: 06.07.2020].

[24] SMOKOWSKI, P. R. y KOPASZ, K. H. (2005). *Bullying in school: An overview of types, effects, family characteristics, and intervention strategies*. Children and Schools. 27 (2): 101-110

datos materia de chantaje suelen ser falsos, sin embargo, al tratarse de personas en edades muy tempranas, sentirán miedo de lo que puedan decir o hacer sus pares si llegan a conocer esta información.

c) Los *rankings* o listas, los cuales siempre han estado presente entre los más pequeños en la modalidad tradicional del acoso, mediante hojas de papel, pero que hoy da un paso más allá, llegando a las redes sociales. Estos *rankings* suelen enumerar en una escala a sus compañeros, generalmente respecto de adjetivos descalificativos, los cuales deben ser comprendidos en el contexto del nivel de madurez de los niños y el contexto en que se desenvuelven, tales como 'feo' o 'tonto', o incluso 'pobre'.

Mediante estos comportamientos, los niños se ven gravemente afectados, puesto que mediante los descalificativos con que se les nombra ven mermada su autoestima, lo cual les dificulta la interacción social con sus pares, en virtud de que comienzan a desarrollar una gran inseguridad en sus relaciones. A su vez, producto de un sentimiento de inferioridad y soledad latente, pueden ver comprometido su rendimiento escolar, o incluso mostrar alteraciones en sus actividades rutinarias, tales como el apetito o el sueño.

d) Intimidación por correo electrónico, o el envío a través de este medio de textos o imágenes abusivos.

e) Hostigamiento en las salas de chat y de videoconferencias.

f) Agresiones a través de sistemas de mensajería instantánea, ya sea persona a persona o persona a un grupo de personas, dentro de las cuales está la víctima.

g) Intimidación a través de sitios web, ya sea ingresando comentarios en sitios web legítimos o creando páginas falsas, en relación con la víctima.

En caso de no atender tempranamente el problema, el menor afectado puede llegar a desarrollar a futuro una personalidad solitaria y sentimientos de inseguridad permanentes, entre otros problemas como la ansiedad o la depresión.

ii.- Formas de prevención del ciberacoso en niños en edad escolar

Se dice que "*en la actualidad, tan solo un 28% de padres aseguran que sus hijos han acudido a ellos con algún problema de acoso escolar*[25]", es por ello por lo que, en caso de sospecha por cambios conductuales del menor, debiera actuarse por los padres o a través de apoyo profesional.

Asimismo, se debe informar al centro educacional en caso de que un menor esté siendo víctima de estas conductas, con el fin de configurar una estrategia en equipo con el personal docente, y que estos últimos puedan estar atentos para evitar nuevas situaciones de ciberacoso y resolver sanamente los conflictos ya existentes entre varios de los alumnos con sus pares.

Otra estrategia de relevancia para evitar el ciberacoso está dada por la formación digital, es decir, se trata de educar también a los padres de los menores en el conocimiento de las nuevas tecnologías, a fin de que manejen correctamente los mecanismos de control parental en los dispositivos digitales y en las redes sociales a las que los niños acceden, restringiendo el acceso de estos a ciertas páginas no recomendables. Del mismo modo, esto debe ser combinado con una constante supervisión de la actividad de los menores en Internet.

Un factor más para la prevención del ciberacoso es la protección de datos, donde se debe mentalizar a estos menores que existe información que no debe ser entregada a nadie, manteniendo de este modo las contraseñas privadas, así como el acceso a ciertos dispositivos en que estén enlazadas cuentas personales utilizadas por dicho menor y que pueda ser usada malintencionadamente por un tercero para suplantarlo.

Finalmente, en los casos más graves de ciberacoso, es posible que los familiares de los afectados quieran recurrir a la vía legal, para lo cual es necesario conocer cuál es la legislación vigente en la materia, tanto en términos generales como las posibles acciones que puedan entablarse para la persecución de las responsabilidades que sean del caso.

[25] ABC Educación. *Muchas víctimas de ciberbullying no acuden a sus familiares a por ayuda*. Madrid, España. 2016. [En línea] en https://www.abc.es/familia/educacion/abci-muchas-victimas-ciberbullying-no-acuden-familiares-ayuda-201612071105_noticia.html [consulta: 10.07.2020].

En los párrafos siguientes será analizado este punto.

7.- Regulación del ciberacoso en Chile

En Chile, el fenómeno del ciberacoso aún no está tipificado como tal, a pesar de que este se da tanto a través de redes sociales como desde aplicaciones de mensajería.

Sin embargo, hasta el momento, existe la tipificación de otros delitos que eventualmente podrían producirse en un contexto de ciberacoso, tales como las amenazas (reguladas en los artículos 296 y siguientes del Código Penal), las injurias (reguladas en los artículos 416 y siguientes del Código Penal), o las calumnias (reguladas en el artículo 412 y siguientes del Código Penal).

En materia laboral, el artículo 2 inciso segundo del Código del Trabajo dispone "*Asimismo, es contrario a la dignidad de la persona el acoso laboral, entendiéndose por tal toda conducta que constituya agresión u hostigamiento reiterados, ejercida por el empleado o por uno o más trabajadores, en contra de otro u otros trabajadores, por cualquier medio, y que tenga como resultado para el o los afectados, su menoscabo, maltrato o humillación o bien que amenace o perjudique su situación laboral o sus oportunidades en el empleo*".

Luego, el inciso cuarto y quinto de ese mismo artículo proscribe los actos de discriminación en el ámbito laboral. Se señala que los actos de discriminación "*son las distinciones, exclusiones o preferencias basadas en motivos de raza, color, sexo, maternidad, lactancia materna, amamantamiento, edad, estado civil, sindicación, religión, opinión política nacionalidad, ascendencia nacional, situación socioeconómica, idioma, creencias, participación en organizaciones gremiales, orientación sexual, identidad de género, filiación, apariencia personal, enfermedad o discapacidad u origen social, que tengan por objeto anular o alterar la igualdad de oportunidades o de trato en el empleo y la ocupación*".

A propósito de estas normas, la Dirección del trabajo, a través del Ord. Nº 3519/34, de 09 de agosto de 2012, se ocupa de precisar algunos de los términos que señala esta ley. Es así como señala que "*la expresión 'hostigamiento' es la 'Acción y efecto de hostigar' y entre las*

acepciones de su infinitivo 'hostigar', se cuentan las siguientes: 'Molestar a alguien o burlarse de él insistentemente' e 'Incitar con insistencia a alguien para que haga algo.

El mismo repertorio léxico define la palabra 'menoscabo' como 'efecto de menoscabar' y, a su vez, respecto de 'menoscabar' contempla, entre otras acepciones 'Causar mengua o descrédito en la honra o en la fama'. A su turno, el concepto "maltrato" como 'Acción y efecto de maltratar', en tanto que su infinitivo 'maltratar' está definido como 'tratar mal a alguien de palabra u obra" y también 'Menoscabar, echar a perder'.

Por último, la expresión humillación está definida por el citado diccionario como 'Acción y efecto de humillar o humillarse y el infinitivo 'humillar', por su parte, como 'herir el amor propio o la dignidad de alguien' y 'Dicho de una persona: pasar por una situación en la que su dignidad sufra algún menoscabo'".

Entendemos que el legislador laboral no distingue respecto de los distintos medios a través de los cuales puede llevarse a cabo la conducta constitutiva de acoso, por lo que perfectamente podría aplicarse estas normas al objeto de nuestro análisis en términos amplios.

Ahora bien, este fenómeno, no está normado en el ámbito de la ley de educación, sin embargo, no ha pasado desapercibido para el Ministerio de Educación y la PDI, quienes han llevado a cabo campañas de concientización y prevención.

No obstante, aunque el ciberacoso no posea una tipificación penal específica, en la actualidad podemos encontrar dos leyes y un proyecto de ley que pretenden incorporar algunas sanciones para hipótesis de agresiones realizadas a través de medios digitales o entre menores, que necesariamente debemos tener a la vista. A continuación, nos referiremos a cada una de ellas:

LEYES	
Ley sobre Violencia Escolar **(Ley Nº 20.536)**	La Ley Nº 20.536, promulgada el 08 de septiembre de 2011, contempla sanciones para alumnos que realicen "*bullying*" al interior de los colegios. Esta Ley introduce modificaciones en el Decreto con Fuerza de Ley Nº 2, del Ministerio de Educación, del año 2010, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 20.370, General de Educación. De esta forma, en el artículo 15 de la Ley Nº 20.370, el cual señalaba que "*En cada establecimiento subvencionado o que recibe aportes del Estado deberá existir un Consejo Escolar. Dicha instancia tendrá como objetivo estimular y canalizar la participación de la comunidad educativa en el proyecto educativo y en las demás áreas que estén dentro de la esfera de sus competencias*[26]", se añade que tal instancia también deberá promover la buena convivencia escolar y prevenir toda forma de violencia física o psicológica, agresiones y hostigamiento. Asimismo, en este mismo artículo, se agrega un tercer inciso que señala lo siguiente: "*Aquellos establecimientos que no se encuentren legalmente obligados a constituir dicho organismo deberán crear un Comité de Buena Convivencia Escolar u otra entidad de similares características, que cumpla las funciones de promoción y prevención señaladas en el inciso anterior. Todos los establecimientos educacionales deberán contar con un encargado de convivencia escolar, que será responsable de la implementación de las medidas que determinen el Consejo*

[26] Ley Nº 20.370, General de Educación. Chile.

	Escolar o el Comité de Buena Convivencia Escolar, según corresponda, y que deberán constar en un plan de gestión[27]". Se agrega también, en su Título Preliminar, un Párrafo 3º, dentro del cual el artículo 16-A describe lo que se entenderá por buena convivencia, describiéndola como la coexistencia armónica de los miembros de la comunidad educativa. Respecto al acoso escolar, dentro del mismo Párrafo 3º, el artículo 16-B señala que el acoso escolar consistirá en toda acción u omisión que constituya agresión u hostigamiento de forma reiterada, ya sea dentro o fuera del establecimiento educacional, realizada por estudiantes que, en forma individual o colectiva, atenten contra otro estudiante, valiéndose de una situación de superioridad o indefensión del estudiante afectado, provoque en este maltrato, humillación o temor fundado de verse expuesto a un mal de carácter grave. Para ello, se contempla que dicha conducta haya sido realizada también por medios tecnológicos o cualquier otro medio. Como sanción al acoso o ciberacoso, esta Ley agrega que, en el caso de que las autoridades del establecimiento no adopten las medidas correctivas, pedagógicas o disciplinarias que su propio reglamento interno disponga, podrán ser sancionadas conforme dispone el artículo 16 de este mismo cuerpo legal, cuya sanción consiste en multas hasta las 50 Unidades Tributarias Mensuales (UTM), las que podrán duplicarse en caso de reincidencia.
Ley contra el "*grooming*"	La Ley Nº 20.526, publicada en el Diario Oficial el 13 de agosto de 2011, sanciona el acoso sexual contra menores.

[27] Ley Nº 20.536, Ley sobre Violencia Escolar. Chile.

(Ley Nº 20.526)	Esta norma introduce diversas modificaciones al Código Penal. Entre ellas, la más relevante modifica el artículo 366 quáter, el cual sanciona con una pena de presidio menor en su grado medio a máximo a quien realizare acciones de significación sexual ante una persona menor de 14 años, tales como hacerlo ver o escuchar material pornográfico o presenciar espectáculos del mismo carácter. La modificación de tal artículo se ve reflejada en el inciso segundo, agregándose sanción penal a la conducta consistente en enviar, entregar o exhibir imágenes o grabaciones de su persona u otro menor de 14 años, con notación sexual, la cual será castigada con presidio menor en su grado máximo. Del mismo modo, la Ley Nº 20.526, en este mismo artículo en análisis, sustituye el tercer inciso por el siguiente: "*Quien realice alguna de las conductas descritas en los incisos anteriores con una persona menor de edad, pero mayor de catorce años, concurriendo cualquiera de las circunstancias del numerando 1º del artículo 361 o de las enumeradas en el artículo 363 o mediante amenazas en los términos de los artículos 296 y 297, tendrá las mismas penas señaladas en los incisos anteriores*[28]". Como inciso cuarto, se contempla la validez de aplicar las sanciones previamente señaladas en los casos en que el delito descrito haya sido cometido a distancia, implementando para ello cualquier medio electrónico.

[28]Ley Nº 20.526, Sanciona el acoso sexual de menores, la pornografía infantil, virtual y la posesión de material pornográfico infantil. Chile.

	Esta ley encuentra su fundamento en la necesidad de que la legislación se adapte a las nuevas realidades que surgen producto del avance de la tecnología.
Art. 403 ter Código Penal	Que sanciona al que sometiere a tratos denigrantes a niños, niñas y adolescentes o a personas en situación de discapacidad
PROYECTOS DE LEY	
Proyecto de Ley que modifica el Código Penal con el propósito de sancionar la difusión no autorizada de material o imágenes con contenido o connotación sexual. **Boletines Nº 11.923-25 y 12.164-07**	Este Proyecto de Ley, que regularía la ley conocida como "*Ley Pack*" busca modificar el Código Penal y aumentar las penas de aquellos delitos que afectan los derechos garantizados por la Constitución, como la protección de la vida privada, sancionando la difusión de fotografías o videos privados de una mujer sin su consentimiento en cualquier plataforma, con multas que van desde las 15 hasta las 20 Unidades Tributarias Mensuales (UTM). De acuerdo a la diputada Maite Orsini, en relación a una investigación de la Fundación Datos Protegidos que arroja como resultado que, hasta enero de 2019, solo a un 7% de las mujeres se les acogió su denuncia por ciberacoso, esta señala que "*ninguna ha concluido en una condena penal o sanción y tampoco ha habido alguna forma de reparación para las víctimas incluso cuando las pruebas incluían la identidad del agresor*[29]". Durante la pandemia mundial causada por el COVID-19, a mitad del año 2020 aproximadamente, en Chile surgió un colectivo denominado '*Leypack ahora*', la cual busca que dicho Proyecto de Ley pueda ver prontamente la luz y sancione penalmente a

[29]ARRIAGADA, Javiera; CALZON, Bernardita. *Ciberacoso: Violencia de género a un solo clic*. Reportaje sobre el acoso y las humillaciones a mujeres en redes y plataformas digitales. Mayo 2019. [En línea] en https://vergara240.udp.cl/ciberacoso-violencia-de-genero-a-un-solo-clic/ [consulta: 17.04.2021].

	aquellas personas que divulguen fotografías íntimas sin la autorización de la persona involucrada, y en consideración a que, si bien los *'pack'* son conjuntos de fotografías sin ropa tomadas voluntariamente, el envío de estas se basan en una relación de buena fe con quien posteriormente procede a divulgarlas con terceros sin consentimiento de la persona afectada.
Mensaje Nº 393-366, de S.E. el Presidente de la República con el que se inicia un proyecto de ley que sanciona el acoso por cualquier medio. **Boletín 12473-07**	Este proyecto de ley considera lo debatido en los proyectos de ley antes señalado, además del proyecto de ley que modifica la Ley Nº 19.223, que tipifica figuras penales relativas a la informática, para tipificar el delito de acoso u hostigamiento por medios informáticos (Boletín Nº 11.801-07). El proyecto de ley, actualmente en primer trámite constitucional, propone los siguientes artículos: "Artículo 1.- *Acoso. Será sancionado con presidio menos en su grado mínimo a medio, el que, contra la voluntad expresa de otra persona, afectando con ello gravemente las condiciones de su vida privada, insistentemente:* *1º la siguiere;* *2º establezca o intentare establecer contacto con ella;* *3º llamare a su teléfono;* *4º le enviare comunicaciones por cualquier medio.* *Si la víctima fuere menos de dieciocho años, se presumirá que existe voluntad contraria cuando lo señalado en el inciso anterior se realizare por cualquier medio electrónico de comunicación*."

	Luego en el artículo 2 se refiere a la difusión no consentida de datos personales o de registros de imágenes o sonidos y en el artículo 3 se refiere a la exhibición y difusión no consentida de material sexual.

Tabla 2

El exsubsecretario de telecomunicaciones y experto en derecho digital, Pedro Huichalaf, se refirió a las dificultades para probar estas conductas, en los siguientes términos: "*el acoso por whatsapp o internet no es constitutivo de delito y es muy difícil de probar ya que muchas veces se usan teléfonos de prepago, por lo que es imposible ubicar al dueño*[30]".

De acuerdo a lo señalado, y al no existir una normativa específica contra el ciberacoso en Chile, las únicas acciones a ejercer consistirían en que, en caso de que se produzcan amenazas reiteradas, se efectúe una demanda por dicho delito, lo cual aplica del mismo modo para los casos en que las declaraciones realizadas sobre una persona mediante redes sociales revistan el carácter penal de injuria o calumnia, entre otros delitos, ya que, de lo contrario, mientras no exista una regulación penal del ciberacoso, muchas conductas que califican como tal tan solo constituirían una falta moral.

Como conclusión para la legislación nacional, podemos señalar que la legislación y los proyectos de ley son más bien escasos, regulándose esto fundamentalmente en otro tipo de normativas, como aquellas que rigen al interior de los centros educacionales en el caso de los menores, o en otro tipo de proyectos de ley que, si bien no se presentan como una "*ley anti-ciberacoso*", sus finalidades están destinadas a evitar ciertas conductas en Internet que podrían ser constitutivas de tal fenómeno, haciéndose cada vez más necesario avanzar en esta regulación.

[30] FUMEY, Juan. *¿Existe una ley que nos proteja del ciberacoso?* Agosto 2018. [En línea] en https://www.bufetes.cl/articulos/existe-una-ley-que-nos-proteja-del-ciberacoso [consulta: 12.07.2020].

8.- Regulación del ciberacoso en derecho comparado

Así como hemos podido constatar que no existe una normativa específica en Chile que regule el ciberacoso, es relevante analizar si otros países han tenido en consideración este tipo de violencia dentro de sus normativas, con énfasis en el ámbito penal. Para ello, se hará una revisión de cuatro legislaciones: la de España, Estados Unidos de América, Perú y Argentina, con la intención de mostrar modelos alternativos.

i.- España

En España, encontramos la tipificación genérica del acoso, el artículo 172 ter, párrafo 1, del Código penal español sanciona a "*el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana*"[31], enunciando un catálogo de conductas típicas.

A continuación, el artículo 173.1 sanciona a quien "*en el ámbito de cualquier relación laboral o funcionarial y prevaliéndose de su relación de superioridad, realicen contra otro de forma reiterada actos hostiles o humillantes que, sin llegar a constituir trato degradante, supongan grave acoso contra la víctima*"[32], de manera que esta norma amplía el ámbito del tipo genérico de acoso, extendiéndolo, por ejemplo, al contexto laboral o de subordinación en general.

Asimismo, junto a este tipo especial de acoso, el artículo 184.1. regula el tipo penal de acoso sexual, penando con privación de libertad al que "*solicitare favores de naturaleza sexual, para sí o para un tercero, en el ámbito de una relación laboral, docente o de prestación de servicios, continuada o habitual, y con tal comportamiento provocare a la víctima una situación objetiva y gravemente intimidatoria, hostil o humillante*[33]". Con este tipo penal se amplía no

[31] Código penal español, artículo 172 ter.
[32] Código penal español, artículo 173.1.
[33] Código penal español, artículo 184.1.

solo el supuesto fáctico que permite configurar el acoso, sino que también precisa los requisitos circunstanciales que le dan lugar.

Así, el Código Penal español regula expresamente las figuras del acoso genérico, el acoso laboral y el acoso sexual, sin referirse expresamente la figura del ciberacoso, sin perjuicio de lo cual debemos considerar que se trata de tipos genéricos que no suponen un medio especial a través del cual pudieran cometerse.

No consideramos que esta normativa específica se refiera a otras especies de hipótesis como el acoso escolar cometido entre alumnos, por cuanto la figura del artículo 173.1 considera el factor de subordinación para su configuración.

Pese a no regular expresamente el ciberacoso, sí regula lo que se ha denominado como *child's grooming*, conducta que se efectúa mediante redes informáticas. En este sentido, el artículo 183 ter.1 del Código Penal español establece una sanción para el que "*a través de internet, del teléfono o de cualquier otra tecnología de la información y la comunicación contacte con un menor de dieciséis años y proponga concertar un encuentro con el mismo*[34]", con la finalidad de cometer ciertos delitos sexuales enunciados por la ley.

Para ciertos autores, esta norma regularía el ciberacoso, refiriéndose que "*tras la Ley Orgánica 1/2015, de 30 de marzo, el delito de ciberacoso que estaba regulado en el art. 183 bis CP, pasa a recogerse en el art. 183 ter que tipifica los actos conocidos como "grooming" o la captación de menores con fines sexuales a través de Internet*[35]".

Sin embargo, de nuestra parte estimamos que parece más preciso decir que la norma regula un subtipo de ciberacoso, caracterizado por su connotación sexual, y no el ciberacoso, propiamente tal.

En este sentido, pese a no existir una consagración expresa del ciberacoso en el Código Penal español, ciertamente el artículo 172 ter, en su párrafo 2°, pareciera sentar las bases de la punición del hostigamiento o acoso cibernético, en tanto establece que será sancionado "*el que*

[34] Código penal español, artículo 183 ter.1.
[35] GUTIÉRREZ, Ainhoa (2019). *Ciberacoso sexualizado y ciberviolencia de género en adolescentes*. Nuevo marco regulador para un abordaje integral. R.E.D.S. núm. 14, (enero- junio). Almería (España), Universidad de Almería. p. 46.

acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana: 2° Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas[36]".

Entendemos que la expresión "*a través de cualquier medio de comunicación*" permite entender que el acoso cometido por medios digitales es punible, pese a no ser exhaustiva la descripción fáctica del tipo penal.

Fuera del ámbito penal, el ciberacoso también ha sido objeto de regulación en el ámbito escolar, a nivel de cada comunidad autónoma. En este sentido, se ha referido que "*todas las comunidades autónomas poseen en la actualidad protocolos específicos para el abordaje del acoso escolar. No sucede igual en el caso del abordaje específico del ciberacoso. De hecho, sólo existe protocolo específico para la actuación ante situaciones de ciberacoso en 3 comunidades: Andalucía, Cataluña, y País Vasco*[37]".

ii.- Estados Unidos de América

Según apunta Christine Weidenlaufer mediante un informe para el comité de Asesoría Técnica Parlamentaria de Chile, en el caso del sistema jurídico estadounidense debe distinguirse entre los niveles federal y estadual. A nivel federal, los conceptos relacionados al ciberacoso son variables. Señala el informe que*:*

"Entre los diversos términos comúnmente utilizados para describir un delito violento en Internet, además del ciberacoso, está el ciber hostigamiento (cyberharassment), ciber acecho (cyberstalking), la ciber extorsión (cyberextortion), la extorsión sexual (sextortion), la venganza pornográfica o pornografía no consensuada (revenge porn/nonconsensual pornography), las ciber amenazas (cyberthreats), entre otros. Estos términos a veces se superponen, lo que aumenta la posible confusión, existiendo asimismo varias posibles vías para enjuiciar estos

[36] Código penal español, artículo 172 ter, párrafo 2°.
[37] VEGA-OSES, A.y PEÑALVA-VÉLEZ, A. (2018). *Los protocolos de actuación ante el acoso escolar y el ciberacoso en España: un estudio por comunidades autónomas*. International Journal of New Education (Universidad de Málaga). Número 1: 51-76.

delitos a nivel federal. Aunque actualmente ninguna ley federal aborda directamente el ciberacoso, en algunos casos, la conducta podría superponerse con el hostigamiento discriminatorio (discriminatory harrassment), cuando éste se basa en la raza, la nacionalidad, el color, el sexo, la edad, la discapacidad o la religión[38]".

Asimismo, la autora señala que, a nivel estadual, si bien los estados han promulgado leyes para prevenir el acoso escolar, pocas se refieren a las formas electrónicas de acoso. Algunos estados criminalizan directamente el ciberacoso, estableciendo sanciones penales como multas e incluso penas de prisión para esta conducta. Pero, por otro lado, muchas conductas de acoso cibernético ya estarían sancionadas penalmente, como a través de las figuras de acoso, acecho, etc.; o civilmente, como la calumnia o la difamación[39].

A nivel federal, el Código 18 de los Estados Unidos, Sección 2261 A se refiere al acoso, incluyendo como medio el correo o cualquier servicio informático interactivo o cualquier instalación de comercio interestatal o extranjero para "*participar en un curso de conducta que cause una angustia emocional sustancial a esa persona o coloca a esa persona en un temor razonable a la muerte o lesiones corporales graves…*" (nos interesa sólo los elementos objetivos del tipo). Asimismo, el acoso como fenómeno genérico se encuentra sancionado en el Título VII del Civil Rights Act de 1964, dedicado especialmente a la sanción de la discriminación. De esta normativa se desprenden conclusiones disímiles para las diversas formas de acoso.

De esta manera, en el ámbito federal y estatal existen diversas normas que recepcionan también un abanico de distintas figuras legales relacionadas con el acoso.

En lo tocante al *bullying*, no existen normas federales que lo sancionen directamente. De esta manera, el tratamiento de este fenómeno a nivel federal guarda relación con el tratamiento de otras conductas sancionadas de carácter más genérico, como lo es el acoso. Así, cuando el acoso se produzca de manera concomitante con hechos constitutivos de *bullying*, especialmente en el ámbito escolar, habrán de aplicarse las normas federales que sancionen el acoso. Entonces, de modo general, las conductas de acoso y *bullying* podrán violar distintas normas de la *Civil*

[38] WEIDENSLAUFER, Christine; MEZA-LOPEHANDÍA, Matías. *El ciberacoso escolar en el derecho penal: Formas de regulación en el derecho extranjero*. 2018. [En línea] en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/25508/1/BCN2018___FINAL___Ciberacoso_en_la_legislacion_extranjera.pdf [consulta: 13.07.2020].

[39] Ibídem.

Rights Law de 1964. Así es señalado por las fuentes electrónicas oficiales del gobierno norteamericano[40].

Lo anterior no obsta de ninguna manera a que los distintos estados hayan establecido, en mayor o menor medida, una normativa especial para regular y sancionar el acoso, especialmente en el ámbito escolar. Así, por ejemplo, en el caso de Washington tenemos que el *Washington Revised Code* establece en su sección 28A.600.477 la prohibición del acoso, la intimidación y el *bullying*, y cuyo apartado 5(b)(1) establece que dichas conductas pueden tener lugar por medios verbales, escritos o electrónicos[41].

En el caso de Nueva York, su *Consolidated Laws* contiene, en materia penal, la sección 240.25 que sanciona acoso en primer grado, y la sección 240.26 que sanciona el acoso en segundo grado[42]. En ninguno de los dos casos se hace referencia al uso de medio electrónicos. En el contexto educacional, este estado cuenta con la S1987B *bill* de 1987, que introdujo modificaciones a la *Education Law*, definiendo en su sección 11(7) el acoso como "*la creación de un ambiente hostil mediante actos o amenazas verbales, intimidación o abuso que tenga, o pueda tener, injustificada o sustancialmente, el efecto de interferir con el desarrollo académico de los estudiantes, oportunidades o derechos, o de su bienestar físico o mental*[43]".

Asimismo, el Estado de Nueva York se encuentra en plena tramitación de la S2318A *bill* que modificará la *Education Law* para contemplar expresamente el fenómeno del *cyberbullying*, mediante la incorporación de la sección 12-A. Esta última contempla penas de hasta un año de presidio para los actos reiterados de *cyberbullying*[44].

Otro ejemplo lo encontramos en el Estado de Oregón, en tanto la sección 339.250 del *Oregon Revised Statue* establece distintos deberes para los alumnos en el ámbito educacional, regulando expresamente los actos constitutivos de amenazas y violencia[45].

---

[40] Stopbullying (Gobierno de Estados Unidos). [En línea] Disponible en https://www.stopbullying.gov/resources/laws/federal. [consulta: 24.05.2021]

[41] Legislatura del Estado de Washington. [En línea]. Disponible en https://app.leg.wa.gov/RCW/dispo.aspx?cite=28A.300.285. [consulta: 24.05.2021].

[42] Senado de Nueva York. [En línea]. Disponible en https://www.nysenate.gov/legislation/laws/CONSOLIDATED. [consulta: 24.05.2021].

[43] Senado de Nueva York [En línea]. Disponible en https://www.nysenate.gov/legislation/bills/2009/S1987/amendment/B. [consulta: 24.05.2021].

[44] Senado de Nueva York https://www.nysenate.gov/legislation/bills/2017/s2318/amendment/a

[45] Legislatura de Oregón. [En línea]. Disponible en https://www.oregonlegislature.gov/bills_laws/ors/ors339.html. [consulta: 24.05.2021].

iii.- Perú

Si analizamos el estado de la cuestión en algunos países latinoamericanos, veremos que el panorama es similar a otros entornos normativos. En el caso de Perú, el ordenamiento jurídico no contempla normas penales que tipifiquen expresamente el ciberacoso como fenómeno genérico, sin perjuicio de lo cual sí hay normas relevantes para nuestro análisis.

En primer lugar, el Código Penal de Perú contempla la figura del acoso genérico en su artículo 151-A, sancionando a quien "*de forma reiterada, continua o habitual, y por cualquier medio, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona sin su consentimiento, de modo que pueda alterar el normal desarrollo de su vida cotidiana*[46]". Respecto a este tipo penal, se ha referido que "*el artículo 151-A del CP presenta una tipología abierta, ya que no está supeditado a una lista de conductas contextualizadas*[47]".

En efecto, el Código Penal de Perú contempla también una figura penal especial, que es la del acoso sexual, establecida en el artículo 176-B, que sanciona a quien "*de cualquier forma, vigila, persigue, hostiga, asedia o busca establecer contacto o cercanía con una persona, sin el consentimiento de esta, para llevar a cabo actos de connotación sexual*[48]".

Enseguida, el mismo artículo 151-A que consagra el tipo de acoso genérico establece otros tipos penales agravados. Uno de estos es establecido en el inciso 3°, que señala que "*igual pena se aplica a quien realiza las mismas conductas valiéndose del uso de cualquier tecnología de la información o de la comunicación*[49]" Aunque la ley no establece el concepto de ciberacoso

---

[46] Código Penal de Perú, artículo 151-A. Disponible en http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/001CD7E6186057450525832800 52F800/$FILE/COD-PENAL_actualizado_16-09-2018.pdf. [consulta: 12.05.2021]

[47] VALLE, Frank (2020). *El acoso genérico como nuevo delito*. En VALLE, Frank *et al* (2020), *Delitos de acoso genérico, acoso y chantaje sexual*. Breña, Pacífico Editores S.A.C. p. 18.

[48] Código Penal de Perú, artículo 176-B. Disponible en http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/001CD7E6186057450525832800 52F800/$FILE/COD-PENAL_actualizado_16-09-2018.pdf.

[49] Código Penal de Perú, artículo 151-A. Disponible en http://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/001CD7E6186057450525832800 52F800/$FILE/COD-PENAL_actualizado_16-09-2018.pdf.

o acoso cibernético se ha entendido por la doctrina que efectivamente es este el tipo penal consagrado.

Así, la doctrina ha descrito las distintas características de este tipo penal, refiriéndose a que la norma en comento consagra tanto la sanción del acoso como del ciberacoso, y que "*el fundamento penológico de la criminalización del "stalker" y del "cyberstalker" no solo debe buscarse en la producción de los referidos hechos materia de exégesis, sino que deberían investigarse en la etiología y en los factores polidisciplinarios que alimentan la aparición de un nuevo delito*[50]".

Además de lo establecido en el Código Penal, tenemos que la Ley Nº 29.719 sanciona el ciberacoso en un ámbito determinado, correspondiente al de la convivencia escolar. El artículo 1° de la Ley Nº 29.719 señala que "*La presente Ley tiene por objeto establecer los mecanismos para diagnosticar, prevenir, evitar, sancionar y erradicar la violencia, el hostigamiento, la intimidación y cualquier acto considerado como acoso entre los alumnos de las instituciones educativas*[51]". Así, tenemos primeramente que el ámbito de la norma se expande a la regulación y sanción del acoso en su expresión más general.

Enseguida, el artículo 6° del mismo cuerpo legal establece el deber de los docentes de "*detectar, atender y denunciar (...) los hechos de violencia, intimidación, hostigamiento, discriminación, difamación y cualquier otra manifestación que constituya acoso entre los estudiantes, incluyendo aquellos que se cometan por medios telefónicos, electrónicos o informáticos*", de manera que, si bien no incluye expresamente la terminología del ciberacoso, de cierto sí contempla en su regulación el acoso cometido mediante medios electrónicos, esto es, el ciberacoso.

Por su parte, el artículo 2º de la Ley Nº 29.719 indica lo siguiente: "*Esta Ley regula la prohibición del acoso escolar, en cualquiera de sus modalidades, cometido por los alumnos entre sí, que provoca violencia y saldo de víctimas*[52]". Esta norma sin duda reafirma la inclusión

[50] PEÑA, Daniel (2020). *El delito de stalker y cyberstalker en el Código Penal Peruano* (Art. 151-A). En En VALLE, Frank et al (2020), *Delitos de acoso genérico, acoso y chantaje sexual*. Breña, Pacífico Editores S.A.C. p. 53.
[51] Ley Nº 29.719. Perú.
[52] Ibídem.

del ciberacoso en su regulación, en tanto establece una prescripción amplia de la prohibición del acoso, incluyéndose los diferentes medios o modos en que tenga lugar.

Los artículos previamente señalados dan muestra de cómo en dicho país la preocupación por la existencia del acoso entre alumnos de las distintas instituciones educativas y sus efectos negativos sobre estos ha llevado a que el tema deba ser regulado legalmente, aunque no necesariamente dentro de un ámbito penal.

En efecto, resulta patente que la regulación establecida por esta ley en comento se aboca al ámbito escolar de manera casi excluyente, sin que alcance a conformar un cuerpo legal punitivo propiamente tal, lo cual puede evidenciarse al analizar los mecanismos que contempla para combatir el acoso. Dentro de los mecanismos para tratar de evitar y erradicar este fenómeno, la misma ley ya citada contempla en su artículo 3º la necesidad de designar un profesional en Psicología al interior de cada institución educativa; el artículo 5° señala como obligación del Ministerio de Educación la de elaborar una directiva clara y precisa, orientada a diagnosticar, prevenir, evitar, sancionar y erradicar la violencia, el hostigamiento y la intimidación entre alumnos; el artículo 6º contempla también la obligación de los docentes y miembros del personal auxiliar de la institución educativa de denunciar inmediatamente ante el Consejo Educativo Institucional los hechos de tal naturaleza que constituyan acoso entre los estudiantes. Es decir, no contempla medidas sancionatorias o penales dentro de los mecanismos de control y prevención del acoso.

De esta manera, tenemos que la legislación peruana regula de manera profusa la figura del acoso, pasando desde la figura penal genérica, hasta el acoso sexual y el ciberacoso, extendiéndose no solo al ámbito estrictamente penal, sino que también abarcando el educacional.

iv.- Argentina

La legislación argentina no habla del ciberacoso en forma expresa, sin embargo, existen diversas disposiciones que regulan temas relacionados a los delitos cibernéticos, contenidas en el Código Penal de la Nación Argentina. En primer lugar, la legislación penal contempla algunas

normas que sancionan de manera especial los daños cometidos mediante sistemas informáticos, específicamente en los artículos 183 y 184. El primero establece la pena en que incurre quien "*alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños*[53]".

Por su parte, el artículo 184 contempla la situación de quien causare daño mediante "*sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía*[54]".

Enseguida, el mismo Código Penal de la Nación Argentina, cuyo Libro II contiene el Título III, que regula los delitos contra la integridad sexual, contiene normas atingentes al tópico en análisis. En efecto, el artículo 131 sanciona a quien "*por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma*[55]".

De esta manera, pese a no tipificarse de manera expresa la figura del ciberacoso, ciertamente sí existe una consideración legal sobre la comisión de ciertos delitos mediante medios informáticos, como en las normas recién citadas. Por ello, parece acertada ciertamente la técnica legislativa asumida, en sentido de abarcar un espectro amplio de situaciones en que el empleo de medios informáticos puede dar lugar a la comisión de delitos. Sin embargo, considerando el principio de tipicidad que rige en materia penal, parece deseable el desarrollo de una tipificación más circunstanciada de las conductas punibles, específicamente con la finalidad de que el ciberacoso sea reconocido como un tipo penal específico, lo que permitiría dar mayor certeza jurídica a las víctimas sobre las acciones que puedan entablarse para su sanción, así como de las garantías de los imputados sobre cuál es la conducta efectivamente punible.

[53] Código Penal de la nación Argentina, artículo 183.
[54] Código Penal de la Nación Argentina, artículo 184.
[55] Código Penal de la Nación Argentina, artículo 131.

9.- El ciberacoso y el Convenio de Budapest

El Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia, o Convenio de Budapest, tiene por objeto el establecimiento de una normativa jurídica de aplicación internacional para la sanción de los delitos informáticos, estableciendo tanto normas de carácter punitivo como procesales, según da cuenta el mismo Convenio.

En lo pertinente al ciberacoso, ciertamente el Convenio no lo trata de manera expresa, no haciéndose uso de dicha terminología, ni regulando hipótesis fácticas que de manera directa puedan subsumirse o categorizarse como ciberacoso. Ello excluye de su ámbito de aplicación aquellas situaciones que efectivamente sean constitutivas de esta categoría de acoso.

Ello por cuanto al tratar y sancionar la comisión de delitos informáticos, es posible constatar que su regulación solo alcanza a aquellos delitos que afecten bienes informáticos como objeto protegido (como el almacenamiento de datos o el abuso de sistemas), excluyendo entonces aquellas conductas cometidas mediante el empleo de medios informáticos, cuando el bien jurídico afectado no es un sistema informático.

Así, parece difícil extender la aplicación del Convenio a la sanción del ciberacoso. En efecto, en virtud de este tratado, los Estados miembros cuentan con la obligación de tipificar delitos contra la integridad de los sistemas o datos informáticos y su contenido, así como poder establecer un procedimiento para la facilitación de la investigación de estos ilícitos. Así, un informe del comité de asesoría técnica parlamentaria del Congreso Nacional de Chile ha referido que:

"*En Chile, los principales incidentes son actividades relativas al phishing, malware y el hackeo de páginas Web gubernamentales, pero también han aumentado las denuncias de grooming y las amenazas contra personas. Nuestro país posee normas como la Ley N°19.223, que tipifica figuras penales relativas a la informática, que resguardan la seguridad del uso de sistemas informáticos, pero en general el sistema legal está desactualizado, o los tipos penales*

están consagrados para otro delito, y la responsabilidad estatal en términos de protección se encuentra compartida en diferentes organismos[56]".

De esta manera, ante la existencia de tales fenómenos delictuales se han generado diversas medidas que buscan combatir la ciberdelincuencia. Entre las medidas penales sustantivas no encontramos ninguna que refiera de manera genérica a la protección de bienes jurídicos afectados mediante bienes informáticos. En lo referente a las conductas que deben tipificarse por el derecho penal sustantivo de los Estados miembros del Convenio de Budapest encontramos las siguientes:

i. Acceso ilícito.
ii. Interceptación ilícita.
iii. Ataques a la integridad de los datos.
iv. Ataques a la integridad del sistema.
v. Abuso de los dispositivos.
vi. Falsificación informática.
vii. Fraude informático.
viii. Delitos relacionados con la pornografía infantil.
ix. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Así, la gran mayoría de estas medidas sustantivas, las que se encuentran entre los números 1° y 6°, buscan establecer medidas de protección respecto de bienes jurídicos relacionados con la integridad de los sistemas informáticos, sin establecer de manera general la protección de otros bienes jurídicos que puedan afectarse mediante su empleo.

Lo anterior queda en evidencia en tanto los números 7° a 9° sí protegen ciertos bienes materiales y jurídicos que trascienden a los sistemas informáticos, como lo son los fraudes cometidos mediante estos, así como los delitos relacionados con la pornografía infantil y la infracción a la propiedad intelectual. Sin embargo, son medidas de carácter específico, de manera que no puede entenderse regulada la afectación a la integridad psíquica que podría

[56] Convenio sobre la Ciberdelincuencia: Convenio de Budapest. Informe Biblioteca del Congreso Nacional de Chile, BCN. Julio 2018.

resultar dañada mediante el ciberacoso. Por ello, parece deseable que los Estados miembros, al momento de recepcionar los deberes emanados del Convenio, puedan no solo incluir la criminalidad cometida en contra de los sistemas informáticos, si no que sancionar, de manera general, los delitos que pueden cometerse mediante ellos.

En cuanto a materia procesal, este Convenio implica la existencia de un compromiso de cada Estado firmante para adoptar las medidas legislativas que sean necesarias para establecer procedimientos que faciliten la investigación y los procesos penales. Estos procedimientos que son:

i. La conservación rápida de datos informáticos almacenados (artículo 16).
ii. La conservación y revelación parcial rápidas de los datos sobre tráfico (artículo 17).
iii. La orden a personas y proveedores de servicios de presentar la información requerida (artículo 18).
iv. El registro de todo tipo de dispositivo o sistema de almacenamiento informático y la confiscación de los datos informáticos almacenados en ellos (artículo 19).
v. La obtención en tiempo real de datos relativos al tráfico (artículo 20).
vi. La interceptación de datos relativos al contenido de las comunicaciones (artículo 21).

Si bien podemos observar que este instrumento no contiene una regulación expresa al tema del ciberacoso, muestra un compromiso por parte de la comunidad internacional en la persecución y sanción de los delitos cometidos en el ámbito cibernético; sin embargo, se hace visible la necesidad de normativa -tanto nacional como internacional-, de incluir este fenómeno dentro del campo penal, para que su sanción pueda ser efectiva y, a su vez, constituya un desincentivo para la población que busca refugiarse en el anonimato de Internet con intención de humillar o menoscabar a terceras personas.

A pesar de no existir mención referente al ciberacoso en el Convenio de Budapest, podemos considerar que este instrumento constituye un antecedente que podría servir de base para la futura creación de nuevos acuerdos internacionales que regulen dichas conductas según los Estados se percaten de la necesidad de introducir una legislación referente a este fenómeno.

CAPÍTULO II. BOTS Y AGENTES ENCUBIERTOS

1. Definición de *bot*

Como señalan los autores Jim Melnick y Ken Dunham, especialistas en robótica, este último de la Universidad de Harvard, la palabra 'b*ot'* proviene de '*robot*', así como la expresión *botnet* proviene del término *robot network*[57]*,* por lo que, como introducción, es necesario hacer una breve mención sobre en qué consiste la robótica, para poder introducir la definición de robot y, por tanto, cuál sería la diferencia fundamental de un *bot* con estos.

En un ámbito jurídico se ha definido a los *bots* aseverando que "*como su nombre indica se trata de un agente policial encargado de investigar y descubrir posibles delitos que se cometen en la red*[58]".

El estudio de los *bots* se enmarca en el desarrollo de una disciplina científica correspondiente a la robótica. Entonces, podemos señalar que la robótica es "*la ciencia que estudia el diseño y la implementación de robots, conjugando múltiples disciplinas, como la mecánica, la electrónica, la informática, la inteligencia artificial y la ingeniería de control, entre otras. Para definirlo en términos generales, un robot es una máquina automática o autónoma que posee cierto grado de inteligencia, capaz de percibir su entorno y de imitar determinados comportamientos del ser humano. Los robots se utilizan para desempeñar labores riesgosas o que requieren de una fuerza, velocidad o precisión que está fuera de nuestro alcance. También existen robots cuya finalidad es social o lúdica*[59]".

Por tanto, como puede sustraerse del párrafo previo, un robot es una máquina configurable por el ser humano para la realización de tareas repetitivas de manera constante, rápida y eficaz. Estas tareas necesariamente estarán enfocadas en el trabajo físico, por ello es

[57] DUNHAM, Ken y MELNICK, Jim (2009). *Malicious Bots: An outside look of the Internet*. Nueva York, CRC Press. p. 1.
[58] CÁNOVAS, Álex (2017). *Agente Encubierto Online*. Tesis de pregrado. Universitat Autònoma de Barcelona. p. 44.
[59] MINISTERIO DE EDUCACIÓN, Argentina. *Presidencia de la Nación. Robótica: Entrá al mundo de la inteligencia artificial*. Conectados, La revista. Argentina. [En línea] https://issuu.com/eslibre.com/docs/rob__tica__entra_al_mundo_de_la_int. [consulta: 09.04.2021].

que son empleados en las industrias automotrices o incluso en las clínicas para la realización de intervenciones quirúrgicas.

De la definición de robot puede intuirse hacia dónde pueden estar enfocadas las tareas de un *bot* y, precisamente, cuál es la característica que lo diferencia de estos robots. Así, Melnick y Dunham refieren metafóricamente que los *bots* "*son abejas obreras altamente adaptables que realizan sus tejidos en una red amplia que está, en el caso de los bots, esparcida en el Internet mundial*[60]". En virtud de lo cual, podemos caracterizarlos como una especie de robot, perteneciente a los *softwares*, que ejecuta diversas funciones en Internet.

Como puede observarse, la principal diferencia entre ambos radica en la existencia o ausencia de un cuerpo físico, así como en las actividades para las que pueden ser programados unos u otros. Mientras que el robot posee un cuerpo físico que les permita desplazarse y realizar labores que impliquen fuerza física, un *bot* es un *software* que se desarrolla en el plano de un sistema informático o Internet, por lo que algunas de sus principales labores para las cuales podrá estar programado consiste en la difusión o recopilación de información en la web.

i.- Finalidad de los *bots*

Si consideramos el amplio espectro de tareas que cumple la robótica en su desarrollo, es posible concluir que los *bots* pueden dar cumplimiento a un sinnúmero de funciones, difícil de precisar. Ello por cuanto su funcionalidad permite desarrollar diversos tipos de tareas en el ámbito digital, según sea el propósito u orientación que se le brinde.

El *bot*, por tanto, también se encontrará presente en un ámbito bastante extenso de funciones, con la diferencia que precisamente los caracteriza y diferencia de los robots: su plano de acción estará siempre en una plataforma electrónica, como en los computadores, y fundamentalmente en Internet. Es por ello que son muy usados en videojuegos y, en general, en el mundo de Internet.

[60] DUNHAM, Ken y MELNICK, Jim (2009). *Malicious Bots: An outside look of the Internet*. Nueva York, CRC Press. p. 1. (Traducción propia).

Así, entre sus diversas funciones se encuentran la creación de sistemas automáticos de inversión en bolsa (*trading bots*) o la creación de sistemas automatizados para la atención de público o funcionamiento de medios de comunicación masiva, como las redes sociales (*chatbots*)[61].

Su origen tiene lugar hace varias décadas, momento en el cual los programadores se percataron de la posibilidad crear programas sencillos para su posterior configuración en la realización de tareas repetitivas de manera más rápida y eficiente que si estas fueran realizadas manualmente por un humano.

Estos *bots* llevan existiendo al menos desde la década de 1990, según consignan Dunham y Melnick, momento en que se habría originado un tipo de *bot* muy masivo, correspondientes a ciertos *malwares* en los sistemas de *Windows*[62]. Sin embargo, con la reciente masificación del uso de Internet y, en consecuencia, de las aplicaciones de mensajería móvil, como *Facebook*, *Messenger* y *Twitter*, son vistos como cada vez con más frecuencia, y en ocasiones su presencia se vuelve cada vez más relevante.

Hoy en día, si bien son utilizados para algunas tareas inocuas como la publicación de contenido en *Twitter*, con el mero objetivo de darle actividad a un perfil mediante mensajes programados, también poseen gran relevancia en cuanto a la difusión de noticias, lo cual puede ser visto como una función positiva, debido a la posibilidad de viralizar con mayor rapidez y a un mayor público una determinada noticia de interés público; como también puede considerarse algo negativo, producto de la existencia de las "*fake news*", o "noticias falsas", donde se les puede dar un uso malicioso a los *bots* para la propagación de contenido que desinforma a la población con el fin de atemorizar a algún determinado grupo de personas, o incluso con intención de promocionar sitios webs fraudulentos.

Además de estas finalidades, los *bots* pueden tener una importancia fundamental en la recopilación de datos, siendo útiles para la realización de estadísticas, así como puede ayudar en la detección y prevención de ciertos fenómenos de Internet. Por ejemplo, en el año 2018,

[61] Ver VARSHNEY, Shekhar (2017). *Building trading bots using Java*. Granges (Suiza). Apress. 283 pp.*;* y RAJ, Sumit (2019). Building chatbots with Python. Karnataka (India) Apress. 205 pp.
[62] DUNHAM y MELNICK, *op. cit.* p. 1.

Mineduc anunció una campaña para prevenir el ciberacoso en redes sociales, la cual contemplaba la incorporación de un *bot* que notifique y tome acciones ante el uso de ciertas palabras que pudieran considerarse ofensivas.

La idea de estos mensajes, según el Mineduc, es que aparecieran en *Facebook*, *Twitter* o *Instagram*, siendo estas las principales redes sociales utilizadas hoy en día, especialmente por los jóvenes.

De acuerdo con lo señalado en el diario "La Tercera", citando a Marcela Cubillos, Exministra de Educación, esta medida tenía como objetivo que los estudiantes "*tomen conciencia del daño y el impacto de las palabras que están usando. (...) Son palabras que son agresivas y discriminadoras. Está estudiado cuáles son las que hacen mayor daño y esas serán detectadas*[63]".

Adicionalmente, la misma Exministra señaló frente a la idea de esta campaña que, al efectuarse este acoso mediante medios tecnológicos, es esencial poder hacer uso de esa misma tecnología para enfrentar el fenómeno, sin embargo, esto no implicaría el almacenamiento de información y datos personales.

Lo que no fue aclarado fueron los alcances del *bot* o los permisos que buscaría obtener para la realización de dichas publicaciones, lo cual es un punto relevante, puesto que podría producirse una eventual invasión a la privacidad en caso de que estos *bots* tuviesen acceso también a mensajes o chats privados en dichas plataformas sin el permiso del usuario de la red social, más allá de los mensajes públicos, y ante la posibilidad de que dichos mensajes, al no contener datos personales, pudiesen ser almacenados o enviados a terceros y pudiesen ser utilizados como una posible prueba en caso de posteriores denuncias por agresiones recibidas mediante estas situaciones de ciberacoso.

Ahora, al margen de las consideraciones científicas o tecnológicas, y analizando el ámbito estrictamente jurídico, creemos que los *bots* juegan un rol primordial en el ámbito de la

[63]La Tercera. *Mineduc crea bot para enfrentar el ciberacoso en redes sociales*. Noviembre 2018. [En línea] en https://www.latercera.com/nacional/noticia/mineduc-crea-bot-para-enfrentar-el-ciberacoso-en-redes-sociales/386876/ [consulta: 17.04.2021].

investigación penal, considerando la influencia que las tecnologías electrónicas e informáticas juegan actualmente en casi todos los ámbitos de la actividad humana.

En efecto, la influencia de la informática en la administración de justicia es cada vez más importante. De ello es reflejo, por ejemplo, la ley Nº 20.886 que, en el caso de Chile, regula la tramitación electrónica de los procedimientos judiciales. Así, se ha llegado a hablar de la justicia electrónica, refiriéndose que "*La e-justicia es la aplicación y la utilización de la información y el conocimiento en la Administración de Justicia. Surge como consecuencia del proceso de incorporación de las tecnologías a los poderes públicos que está teniendo lugar en las últimas décadas*[64]".

ii.- Regulación del empleo de *bots* en Chile

Hasta el presente año 2021, en Chile no existe regulación expresa que se encargue de regular el alcance y profundidad de la labor de los *bots* en Chile, es decir, no se cuenta con una normativa que señale las restricciones de privacidad que estos tendrían a la hora de promocionar o recabar cierta información, según el fin específico para el que se emplee el *bot*; menos aún se ha previsto qué eficacia jurídica podría tener la información detectada por estos en el caso de que, ante una eventual vulneración de derechos por parte de un usuario de Internet -más específicamente de las redes sociales- hacia un tercero, quisiese hacerse uso de esta información obtenida por un *bot* como medio probatorio ante los tribunales de justicia.

Del mismo modo, al no existir normativa sobre los límites de actuación de los *bots*, surge la interrogante de en quién recaería la responsabilidad penal en caso de producirse una intromisión en la privacidad de los usuarios afectados por la implementación de esta medida intrusiva. ¿Sería atribuible dicha responsabilidad al desarrollador del *bot*, al incluir en él la capacidad de detectar y almacenar cierta actividad en chats privados; o sería responsabilidad del dueño de la red social en la cual se emplee, en caso de que este haya dado su consentimiento para la actuación de esta herramienta en el sitio web donde se cometa la vulneración?

[64] HERNÁNDEZ, María (2019). *Inteligencia artificial y Derecho penal*. En Actualidad Jurídica Iberoamericana Nº 10 bis, junio. España, Instituto de Derecho Iberoamericano. p. 805.

Como puede observarse, quedan en el aire múltiples interrogantes de las que la normativa chilena no se ha hecho cargo hasta el momento, a pesar de que la existencia de los *bots* en las redes sociales es hoy una realidad, y cuyo protagonismo aumenta cada día más, debido a la gran gama de funciones que estos pueden llevar a cabo, por lo que es plausible la búsqueda de una respuesta, toda vez que la posibilidad de que los *bots* realicen la labor de detección de situaciones constitutivas de ciberacoso puede vislumbrarse cada vez más en el futuro. Prueba de ello es la ya mencionada campaña que Mineduc presentó en Chile en el año 2018, cuyo plan "*contempla la creación de un bot o sistema que envía mensajes predefinidos cuando encuentra palabras para las que fue programado. El proyecto incluye que cuando se detecte una falta, se posteará en los muros de los usuarios uno de los cuatro videos con testimonios contra el ciberacoso (podrán aparecer en Facebook, Twitter o Instagram)*[65]", aunque esta iniciativa aún no haya sido concretada hasta el presente.

iii.- Regulación del empleo de *bots* en derecho comparado

Como ya se adelantara en páginas previas, los *bots* llevan existiendo ya varias décadas entre los usuarios de Internet, sin embargo, es más reciente su masificación, lo que podría justificar que la regulación de estos programa computacional sea casi inexistente en la mayor parte de las legislaciones, no habiendo total claridad respecto a qué es lo que tienen permitido hacer y a quién se le podría atribuir la responsabilidad en caso de que estos cometiesen una vulneración de derechos de algún usuario en las llamadas redes sociales.

En este contexto, cabe mencionarse que, si de por sí la regulación de los *bots* no ha sido un tema muy tocado en la mayoría de los estados, menos probable será encontrar ley que haga referencia al empleo de estos en temas relacionados al ciberacoso, pero será de interés revisar algunas propuestas ofrecidas en distintos países respecto al empleo de robots, por lo que se analizará a continuación el trato que ha recibido el tema en la Europa (específicamente dentro de la Unión Europea) y en Japón.

[65] NAVARRETE, María José. *Mineduc crea bot para enfrentar el ciberacoso en redes sociales.* La Tercera. 04 de noviembre de 2018. [En línea] en https://www.latercera.com/nacional/noticia/mineduc-crea-bot-para-enfrentar-el-ciberacoso-en-redes-sociales/386876/ [consulta: 17.07.2020].

a.- Europa

En el plano supranacional, existen algunas directrices que permiten sentar las bases para el desarrollo normativo de una regulación jurídica general y amplia sobre robótica. En este sentido, tenemos que la Resolución del Parlamento Europeo, de 16 de febrero de 2017, establece recomendaciones generales a una de sus comisiones especiales, que es la Comisión sobre normas de Derecho civil sobre robótica[66].

Entre los diferentes aspectos jurídicos concernientes al desarrollo de la robótica tenemos que la resolución trata temas como la responsabilidad civil, la propiedad intelectual, el empleo de vehículos autónomos, el uso médico de robots, entre otras relacionadas con el desarrollo y aplicación de estas tecnologías.

En cuanto a la responsabilidad, el considerando plantea que el marco jurídico vigente en la Unión Europea no es suficiente para regular los daños cometidos por el desarrollo de las nuevas tecnologías caracterizadas por su autonomía y posibilidad de aprendizaje. Es por esta razón que en el numeral 49 de la resolución se recomienda abordar la regulación de estos daños a nivel del Parlamento Europeo. En específico, propone que la regulación de la responsabilidad deberá considerar tanto el grado de autonomía existente en la tecnología, así como el grado de incumbencia de los desarrolladores en la actuación de estas máquinas; recomendando establecer de manera expresa si se adoptará un sistema de responsabilidad civil estricta o no.

Quizás uno de los aspectos más interesantes es el de acuñar el concepto de persona electrónica, como una posible técnica jurídica para determinar el estatuto de la responsabilidad civil en el marco de la robótica e inteligencia artificial. Todo lo cual, ha abierto un flanco de discusión hacia la expansión del concepto de personalidad jurídica.

Con todo, hasta el año 2019 no se habían presentado mayores avances en estas materias. Así lo evidencia Resolución del Parlamento Europeo, de 12 de febrero de 2019, sobre una política industrial global europea en materia de inteligencia artificial y robótica, que, si bien celebra la propuesta de crear un comité de expertos para legislar en materias de robótica, también

[66] Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica. Disponible en el sitio de Internet del Parlamento Europeo, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html#title1.

lamenta que a la fecha no se hubiera presentado ninguna propuesta legislativa referente a la materia, como consta en su numeral 131[67].

En la Revista Jurídica de la Universidad de León, en España, María José Santos señala que: "*La tecnología ha pasado por diversas fases, una primera en que las personas se conectaban a internet, posteriormente, a través de internet y ahora estamos en la fase de que son las cosas las que conectan a internet para mejorar la vida de las personas. La siguiente fase, que es inminente, va a consistir en que las cosas (robots) interactúen con el entorno de manera autónoma e independiente del control humano, con la posibilidad de que incluso las personas se combinen con robots para mejorarse (cyborg)*[68]".

Señala también que: "*A nivel Europeo la Estrategia global para la política exterior y de seguridad de 2016 de la Unión Europea recoge la necesidad de disponer de "normas mundiales en ámbitos tales como la biotecnología, la inteligencia artificial, la robótica y los aparatos pilotados a distancia, con el fin de evitar riesgos de seguridad y aprovechar sus beneficios económicos". En todos estos ámbitos, la UE pretende promover intercambios de información en los foros multilaterales pertinentes con el fin de encabezar la formulación de normas y crear asociaciones en aquellos ámbitos que se encuentran en los confines de la reglamentación multilateral. El primer paso importante a nivel europeo ha sido la elaboración de un informe el 31 de mayo de 2016 en que se recogen recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica*[69]".

Profundizando en el estado de la legislación española sobre robótica, la mentada autora analiza diversas áreas del Derecho en que es necesario el desarrollo de una legislación que recoja las problemáticas jurídicas más relevantes en el tráfico tecnológico y robótico, reflexiones desde las que es posible desprender que en su estado actual el Derecho español no cuenta con una

[67] Resolución del Parlamento Europeo, de 12 de febrero de 2019, "*sobre una política industrial global europea en materia de inteligencia artificial y robótica*". Disponible en el sitio de Internet del Parlamento Europeo, https://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_ES.pdf.
[68] SANTOS, M. (2007). *Regulación legal de la robótica y la inteligencia artificial: retos de futuro*. Revista Jurídica de la Universidad de León.4: 25-50. p. 25.
[69] Ibídem. p. 26.

regulación que recoja expresa ni orgánicamente el tratamiento legal que ha de recibir la robótica ni la inteligencia artificial.

En este mismo sentido, refiere la autora que algunas de las problemáticas jurídicas a que da lugar el desarrollo de las tecnologías robóticas corresponden al estatuto de la responsabilidad civil, contractual y aquiliana; la responsabilidad por producción defectuosa de robots, el almacenamiento de datos y la ciberseguridad, entre otras.

Respecto a la responsabilidad civil, la autora señala que en la actual legislación española no es posible señalar a los robots como sujetos de Derecho, en tanto "e*n el actual marco jurídico, los robots no pueden ser considerados responsables de los actos u omisiones que causan daños a terceros*[70]", agregando que la falta de voluntad existente en estas máquinas dificulta la atribución de responsabilidad, al tiempo que impide establecer el vínculo de causalidad entre un hecho ilícito y el daño. Por ello, estimamos que, en esta materia, mientras la inteligencia artificial no alcance una autonomía más avanzada, es necesario que se precise cuál de los intervinientes en la producción y uso de los robots habrá de responder por los daños ocasionados en el desarrollo de sus funciones.

Finalmente, en lo tocante a la responsabilidad penal, la autora concluye que "*se deberá estudiar si un robot puede actuar con intencionalidad o con dolo. Al fin y al cabo, sus decisiones son fruto de algoritmos y probabilidades*[71]", todo lo cual se condice con los fundamentos del Derecho punitivo, así como es coherente con atender el desarrollo real de la robótica y la capacidad intelectual que los robots puedan alcanzar. En el intertanto, se estima razonable la aplicación de las leyes generales, considerados los robots como medios en la comisión de ilícitos punibles.

Por todo lo anterior, cabe concluir que en el caso de España el desarrollo legislativo sobre robótica es prácticamente inexistente. No existe una ley marco sobre la materia ni tampoco normas especiales que regulen la aplicación de estas tecnologías, en virtud de lo cual resulta necesario adecuar las leyes existentes a la aplicación de estas, junto con la necesidad imperiosa

[70] SANTOS, M. (2007). *Regulación legal de la robótica y la inteligencia artificial: retos de futuro*. Revista Jurídica de la Universidad de León.4: 25-50. p. 37.
[71] Ibídem. p. 39.

de avanzar en un desarrollo jurídico que dé respuesta a los avances actuales e inminentes de la robótica e inteligencia artificial, inclusos los *bots*, como especie de robots.

Sin perjuicio de ello, advertimos que la ley de enjuiciamiento criminal (LECRIM) española sí concibe en su regulación la incorporación de probanzas electrónicas. Así, se ha referido que "*por lo que respecta a la prueba electrónica, con carácter general se aplica el segundo de estos sistemas, en virtud del artículo 384.3 LEC, que permite que el Tribunal valore los medios de prueba conforme 'a las reglas de sana crítica'*[72]". Norma que, a nuestro juicio, otorgaría un espectro amplio de posibilidades en cuanto al desarrollo de pruebas informáticas, incluido el uso de *bots* como medio de investigación.

b.- Japón

Pese a que las naciones asiáticas participan de tradiciones jurídicas distantes a los sistemas occidentales, ciertamente los avances tecnológicos en materia de robótica también han dado lugar a diferentes desafíos jurídicos.

En este sentido, los estudios de la autora Carmen Tirado han arrojado que no existe en la legislación japonesa una definición jurídica única en materia de robótica[73]. Así, la legislación japonesa ha tenido distintas definiciones de lo que es un robot, parceladas en distintos ámbitos jurídicos, como el propio del desarrollo industrial o las relaciones laborales. Así, por ejemplo, el Comité de Normas Industriales de Japón habría desarrollado distintas definiciones de lo que debía entenderse por robot en materias industriales en los años 1979, 1998 y la más reciente del año 2015.

Finalmente, la autora concluye que al existir distintas definiciones jurídicas sectoriales que buscan precisar lo que es un robot en ámbitos determinados, el desafío jurídico en Japón estriba en alcanzar una definición que pueda aplicarse a las distintas ramas del Derecho. Así, las

[72] HERNÁNDEZ, María (2019). *Inteligencia artificial y Derecho penal*. En Actualidad Jurídica Iberoamericana Nº 10 bis, junio. España, Instituto de Derecho Iberoamericano. pp. 792-843. p. 815.
[73] TIRADO, Carmen (2020). *¿Qué es un robot? Análisis jurídico comparado de las propuestas japonesas y europeas*. En Mirai, Estudios japoneses (Universidad Complutense de Madrid). 4: 35-48. p. 35.

definiciones dadas en el contexto industrial, por ejemplo, no permiten resolver las problemáticas sobre responsabilidad penal a que puede dar lugar la robótica[74].

2.- Los agentes encubiertos

En el ámbito de la investigación criminal, el proceso penal contempla diversas técnicas investigativas según los supuestos de hecho a que dé lugar la investigación de los distintos tipos penales. Así, por ejemplo, entre algunas de las técnicas especiales de investigación en Chile encontramos la interceptación de medios de comunicación, el allanamiento de distintos tipos de edificios o la función del agente encubierto.

En particular, el medio investigativo del agente encubierto guarda relación con la necesidad de investigar cierto tipo de delitos como lo son, particularmente, los cometidos a través de organizaciones criminales, en que el seguimiento de una línea de investigación particular resulta compleja, especialmente para la producción de medios de prueba que puedan aportarse ante un tribunal.

Así, tratándose de su conceptualización, se ha definido al agente encubierto "*como un funcionario de la policía que se infiltra en una organización criminal, cambiando de identidad, llevando a cabo tareas principalmente de represión y de prevención del delito, con el fin de ganarse la confianza del grupo, identificar a sus integrantes, obtener información en cuanto a su funcionamiento, financiación, etc., recaudar pruebas y, excepcionalmente, presentar testimonio de cargo ante la justicia*[75].

Debido a la eficacia que supone el tener un agente policial encubierto en una organización criminal frente a la dificultad de cualquier otro tipo de investigación ante los delitos señalados previamente, la figura del agente encubierto ha sido reconocida e incorporada en las legislaciones de gran parte de los países del mundo, tanto así que podemos identificar distintas definiciones de agente encubierto realizadas por autores de diversas nacionalidades.

El autor argentino José Caffarena define al agente encubierto como: "*un funcionario*

[74] TIRADO, Carmen (2020). *op. cit*. p. 40.
[75] RIQUELME, E. *op. cit*., p. 8; MONTOYA, M. *op. cit*., p. 79, 153; RENDO, Á. o*p. cit.*; y ARCINIEGAS, G. *op. cit*., p. 317

público que fingiendo no serlo (simulando ser delincuente) se infiltra, por disposición judicial, en una organización delictiva (por ejemplo, de narcotraficantes), con el propósito de proporcionar "desde adentro" información que permita el enjuiciamiento de sus integrantes y, como consecuencia, el desbaratamiento de esa asociación ilícita[76]".

En Perú, Alonso Peña lo define como: "*una práctica estatal particularmente comprendida en el ámbito de la criminalidad organizada, a fin de combatir las mafias del narcotráfico y las organizaciones subversivas; son efectivos policiales "especializados", quienes se infiltran en dichas estructuras criminales, bajo identidades falsas, participando activamente en sus actividades ilícitas, a fin de adquirir evidencias suficientes de criminalidad y así poder desbaratarlas. Para tales efectos se le considere identidades supuestas, pero su rol –para ser legítimo, mejor dicho, justificado- debe circunscribirse a ciertos parámetros legales*[77]".

Por su parte, para el magistrado español Francisco Soto, el agente encubierto podría definirse como: "*aquel sujeto, ordinariamente integrado en la fuerza pública, que, con el designio de llegar a descubrir una conducta delictiva en marcha o en desarrollo, lleva a término un despliegue actuacional que, sorprendiendo al abordado infractor, saca a la luz su comportamiento incriminable*[78]".

En la legislación chilena, el agente encubierto se encuentra regulado en la Ley Nº 20.000, que sustituyó a la Ley Nº 19.366, que sanciona el tráfico ilícito de estupefacientes y sustancias psicotrópicas. La definición de agente encubierto se encuentra en artículo 25, inciso 2º de dicha ley, el cual señala que: *"Agente encubierto es el funcionario policial que oculta su identidad oficial y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones con propósitos delictivos, con el propósito de identificar a los partícipes, reunir información y recoger antecedentes necesarios para la investigación...*[79]".

Por otro lado, el oficio reservado Nº 271, del 03 de junio del 2002, del Ministerio Público, que comentaba modificaciones introducidas por la Ley Nº 19.806 al artículo 34 de la

[76] CAFFERATA, J. (2003). *La prueba en el proceso penal* (5º edición). Buenos Aires, Editorial Depalma. p. 223.
[77] PEÑA, A. (2011). *El nuevo proceso penal peruano*. Lima, Gaceta Jurídica. p. 145.
[78] SOTO, F. (1989). *El delito de tráfico ilegal de drogas*. Madrid, Editorial Trivium S.A. p. 31.
[79] Ley Nº 20.000, Ley de Drogas. Chile.

Ley Nº 19.366 sobre agente encubierto, y el cual quedó sin efecto por el oficio N°061, del 30 de enero de 2009, conceptualizaba al agente encubierto como: "*aquella técnica investigativa que permite penetrar desde afuera una organización dedicada al tráfico ilícito de estupefacientes y sustancias psicotrópicas, a través de la infiltración de un agente con la finalidad de obtener información para desbaratarla...*".

De este repertorio de definiciones, tanto doctrinarias como legales, podemos caracterizar entonces al agente encubierto como un miembro de la policía que, mediante la ocultación de su identidad real y bajo una actitud representada, procede a infiltrarse en una organización criminal, con el objeto de convencer a los miembros de esta organización de un supuesto interés en la obtención de ganancias que se derivan de esta actividad delictual, pero con la real intención de investigar desde dentro de dicha organización y aplicar sus conocimientos legales para reunir los antecedentes necesarios que permitan a la justicia atribuir responsabilidad jurídica a los partícipes que infringen la ley.

Como puede extraerse de esta descripción, los elementos que van a caracterizar entonces la actuación de un agente encubierto son los siguientes:

1. Un agente policial cuya identidad es oculta.
2. Que se trate de delitos realizados por el crimen organizado.
3. La introducción de este agente policial en la organización criminal.
4. La realización de una investigación con el objeto de identificar a quienes participan del ilícito que se investiga para obtener pruebas en su contra.

i.- Origen del agente encubierto

La figura del agente encubierto tiene un origen incierto, toda vez que se desconoce exactamente en qué momento de la historia surge, sin embargo, existe cierto consenso en la doctrina de que esta podría tener su origen con la llegada de las monarquías absolutistas europeas, fundamentalmente en Francia mediante el llamado "*agent provocateur*" ("agente

provocador"), el cual, a su vez, sería una evolución de la figura del "delator".

El autor Juan Muñoz, quien forma parte de la doctrina mayoritaria que posiciona el nacimiento del agente provocador con el absolutismo francés, señala que primeramente habría surgido la figura del delator, "*compuesta por ciudadanos que descubrían a los enemigos políticos para recibir favores del príncipe. En esta época su actividad se limitaba a espiar y poner los hechos en conocimiento de la autoridad, sin que se realice una actividad de provocación. Con el paso del tiempo, la actividad de vigilar no sería suficiente para neutralizar la oposición al régimen y se pasa del espionaje a la provocación*[80]".

El agente provocador, por su parte, puede definirse como aquel que "*provoca la comisión de un hecho como medio necesario para conseguir la reacción en el sentido deseado. Cuando incita a otro a cometer un delito no lo hace con el fin de lesionar o poner en peligro el bien jurídico afectado, sino con el propósito de que el provocado se haga acreedor a una pena*[81]".

Por tanto, este agente induce a otro a cometer un delito, contribuyendo así a su ejecución mediante actos de coautoría, con el fin de lograr que este obtenga sanción por su conducta.

Como salta a la vista, la figura del agente encubierto y la del agente provocador pueden aparejar consecuencias procesales distintas en materia probatoria. Así, la prueba recabada mediante el empleo del agente encubierto provocador puede dar lugar a alguna hipótesis de prueba ilícita o ilegal, por cuanto se propicia la comisión de algún delito con la finalidad de dar éxito a la persecución criminal, mediante lo cual pueden verse afectados distintos derechos fundamentales, ya sustanciales o procesales.

Hoy día, la figura del agente encubierto se hace presente en la mayoría de legislaciones, puesto que se consolida como un método eficaz para combatir el crimen organizado. En lo sucesivo, revisaremos los fundamentos de esta técnica investigativa, así como de su evolución y la incidencia de los medios tecnológicos modernos en su desarrollo.

[80] MUÑOZ, J. (1995). *La moderna problemática jurídico penal del agente provocador*. Valencia, Tirant lo Blanch. p. 21.
[81] RUIZ ANTÓN, Luis Felipe (2015). *El agente provocador*. Tesis doctoral, Universidad Complutense de Madrid, Facultad de Derecho. Madrid, España. p. 31.

ii.- Fundamentos de la figura del agente encubierto

En base a lo expuesto sobre el agente encubierto y respecto a los delitos en que procede su actuación, puede evidenciarse que ante un fenómeno como lo es el crimen organizado, no bastará para su investigación los medios tradicionales, "*de ahí que ante una situación como la que hemos descrito y de las dimensiones y peligrosidad indicadas, debemos acudir a medios de investigación extraordinarios o extremos, se califican así aquellos que pueden suponer una alteración de los principio reguladores del proceso justo, pero siempre con control judicial y respeto, como límite, a la garantía de los derechos fundamentales constitucionalmente reconocidos*[82]".

En tal sentido, pareciera ser que el fundamento general para la consagración del agente encubierto en las distintas legislaciones dice relación con la necesidad de investigar delitos o crímenes especialmente complejos o que afecten bienes jurídicos con mayor intensidad. Por ello, la justificación y necesidad de esta técnica investigativa dirá relación con las características especiales del delito en específico para el cual fue concebido, ya sea la investigación de crímenes de tráfico de estupefacientes, el tráfico de personas u otro tipo de investigaciones criminales.

En palabra del profesor español Emiliano Borja, y en base a la definición de política criminal de Claus Roxin: "*La Política Criminal es una disciplina que se estructura en torno a la estrategia de lucha contra el crimen […]. Su función va más allá, alcanza al tratamiento de la problemática de los ciudadanos que perpetran hechos delictivos […]. Es una disciplina que se encuentra entre la ciencia y la política […]. Su metodología se desarrolla entre el ámbito de la elaboración teórica y el plano de su incidencia práctica en la realidad social […]*[83]".

Dicho de otro modo, y en palabras simples, la política criminal consiste en la estrategia que adopta el Estado para enfrentar el fenómeno de la criminalidad, por lo que cada sociedad tendrá una política criminal diferente de acuerdo con su realidad y a sus propias necesidades, la

[82] DEL POZO, M. (2006). *El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal Española*. Criterio jurídico, 6: 267-310. p. 280.
[83] BORJA, E. (2003). *Sobre el concepto de política criminal. Una aproximación a su significado desde la obra de Claus Roxin*. Anuario de derecho penal y ciencias penales (España). 56(1): 113-150. p. 121.

cual justificará el empleo del agente encubierto o no ante ciertos delitos.

iii.- Regulación del agente encubierto en Chile

El artículo 226 bis del Código procesal penal chileno regula el uso de las técnicas especiales de investigación. Su inciso 1º regula los requisitos de la técnica investigativa de interceptación de comunicaciones telefónicas, regulada en el artículo 222 del mismo Código. Enseguida, el inciso 2º del artículo 226 bis regula el empleo de otras técnicas investigativas, correspondientes a las entregas vigiladas y controladas, así como los agentes encubiertos. Finalmente, su inciso 3º consagra la figura del agente revelador.

De esta manera, los requisitos legales que establece la legislación procesal penal para que sea procedente el uso del agente encubierto corresponden a los siguientes: (a) que se trate de alguno de los tipos penales taxativamente referidos en la ley, esto es, los contemplados en la Ley Nº 17.798, el establecido en el artículo 190 de la Ley Nº 18.290 y en los artículos 442, 443, 443 bis, 447 bis, 448 bis y 456 bis A del Código Penal; los crímenes contemplados en los artículos 433, 434, 436 inciso 1º, y 440 del Código Penal; así como de los delitos previstos en la Ley Nº 20.000 cuando sea procedente; (b) que su empleo fuere necesario para lograr el esclarecimiento de los hechos, (c) necesario para establecer la identidad y participación de las personas determinadas en la investigación, (d) que tenga por propósito conocer y prevenir la planificación delictual; y (e) que exista autorización judicial, conforme al inciso 4º del artículo 226 bis del Código Penal.

El ejercicio de la técnica especial de investigación del agente encubierto queda sujeta a los preceptuados en los artículo 23 y 25 de la Ley Nº 20.000, que sustituye la Ley Nº 19.366, que sanciona el tráfico ilícito de estupefacientes. De este modo, con la nueva ley, el agente encubierto pasa a ser regulado en el párrafo 3º del título II de la Ley Nº 20.000, el cual se titula: *"Del agente encubierto, del agente revelador y del informante"*.

En este título II, el art. 25 describe las tres figuras de la siguiente forma: *"El Ministerio Público podrá autorizar a funcionarios policiales para que se desempeñen como agentes encubiertos o agentes reveladores y, a propuesta de dichos funcionarios, para que*

determinados informantes de esos servicios actúen en alguna de las dos calidades anteriores.

Agente encubierto es el funcionario policial que oculta su identidad oficial y se involucra o introduce en las organizaciones delictuales o en meras asociaciones o agrupaciones con propósitos delictivos, con el objetivo de identificar a los participantes, reunir información y recoger antecedentes necesarios para la investigación.

El agente encubierto podrá tener una historia ficticia. La Dirección Nacional del Servicio de Registro Civil e Identificación deberá otorgar los medios necesarios para la oportuna y debida materialización de ésta.

Agente revelador es el funcionario policial que simula ser comprador o adquirente, para sí o para terceros, de sustancias estupefacientes o psicotrópicas, con el propósito de lograr la manifestación o incautación de la droga.

Informante es quien suministra antecedentes a los organismos policiales acerca de la preparación o comisión de un delito o de quienes han participado en él, o que sin tener intención de cometerlo y con conocimiento de dichos organismos, participa en los términos señalados en alguno de los incisos anteriores.

El agente encubierto, el agente revelador y el informante en sus actuaciones como agente encubierto o como agente revelador, estarán exentos de responsabilidad criminal por aquellos delitos en que deban incurrir o que no hayan podido impedir, siempre que sean consecuencia necesaria del desarrollo de la investigación y guarden la debida proporcionalidad con la finalidad de la misma".

Como puede observarse en el inciso final de este artículo 25, la norma no solo describe la figura del agente encubierto -en conjunto con la del agente revelador y el agente informante- sino que también lo exime expresamente de responsabilidad penal cuando este actúa autorizado por el Ministerio Público, respecto de los ilícitos que estos necesariamente deban realizar o estén impedidos de evitar para el logro del éxito de la investigación. Sin embargo, la parte final de este inciso también hace mención a la debida proporcionalidad que estos actos deben guardar con la finalidad de dicha investigación, toda vez que, si este agente excede sus atribuciones al actuar, será factible analizar la ausencia de antijuridicidad en sus actos.

Asimismo, tenemos que el Código penal chileno también contempla una situación especial en que es procedente la utilización del agente encubierto, como técnica investigativa especial, cual es el caso de ciertos delitos sexuales que afecten a menores de edad. Así, el artículo 369 ter del Código penal establece que:

"Cuando existieren sospechas fundadas de que una persona o una organización delictiva hubiere cometido o preparado la comisión de alguno de los delitos previstos en los artículos 366 quinquies, 367, 367 ter, 374 bis, inciso primero, y 374 ter, y la investigación lo hiciere imprescindible, el tribunal, a petición del Ministerio Público, podrá autorizar la interceptación o grabación de las telecomunicaciones de esa persona o de quienes integraren dicha organización, la fotografía, filmación u otros medios de reproducción de imágenes conducentes al esclarecimiento de los hechos y la grabación de comunicaciones. En lo demás, se estará íntegramente a lo dispuesto en los artículos 222 a 225 del Código Procesal Penal.

Igualmente, bajo los mismos supuestos previstos en el inciso precedente, podrá el tribunal, a petición del Ministerio Público, autorizar la intervención de agentes encubiertos. Mediando igual autorización y con el objeto exclusivo de facilitar la labor de estos agentes, los organismos policiales pertinentes podrán mantener un registro reservado de producciones del carácter investigado. Asimismo, podrán tener lugar entregas vigiladas de material respecto de la investigación de hechos que se instigaren o materializaren a través del intercambio de dichos elementos, en cualquier soporte.

La actuación de los agentes encubiertos y las entregas vigiladas serán plenamente aplicables al caso en que la actuación de los agentes o el traslado o circulación de producciones se desarrolle a través de un sistema de telecomunicaciones.

Los agentes encubiertos, el secreto de sus actuaciones, registros o documentos y las entregas vigiladas se regirán por las disposiciones de la ley Nº 20.000".

Como puede observarse, el artículo 369 ter del Código Penal dispone que la actuación de los agentes encubiertos será plenamente aplicable en caso de que la circulación de producciones se desarrolle a través de un sistema de telecomunicaciones, es decir, este artículo hace extensivo el terreno de actuación de los agentes encubiertos al campo informático, pero

puede fácilmente deducirse que funciona como complemento respecto de la investigación de aquellos delitos taxativos en que se permite accionar a un agente encubierto, puesto que no regula la implementación de dicha medida a otro tipos de conductas, tales como el ciberacoso, discursos de odio o amenazas mediante redes sociales y servicios de mensajería.

Por otro lado, si bien los agentes encubiertos están regulados en leyes penales especiales, en algunas disposiciones del Código Penal y en el Código Procesal Penal, cabe destacarse que estas suelen referirse a los agentes encubiertos en el plano físico. Adicionalmente, también es relevante señalar que la implementación de estas medidas se encuentran restringidas a ciertas y determinadas materias, tales como el tráfico ilícito de drogas y otros estupefacientes; o la elaboración, distribución o posesión de pornografía infantil. Por ello, la especialidad de esta técnica de investigación guarda también directa relación con la excepcionalidad de su empleo. Todo lo cual nos llevará a preguntarnos si, además de su procedencia, la ley regula también de manera estricta los medios en que puede consistir su ejercicio, esto es, si puede el agente encubierto corresponder únicamente a personas naturales u otras formas de tecnología.

iv.- Regulación del agente encubierto en derecho comparado

Como se analizará en las próximas líneas, la técnica del agente encubierto está presente en la legislación penal de diversos países. Con todo, en cada uno de ellos presenta algunas particularidades, especialmente en relación con el tipo de delitos para cuya investigación fue incorporado este mecanismo de investigación.

a. España

El artículo 282 bis del Código procesal español establece en su inciso 1º que "*el Juez de Instrucción competente o el Ministerio Fiscal dando cuenta inmediata al Juez, podrán autorizar a funcionarios de la Policía Judicial, mediante resolución fundada y teniendo en cuenta su necesidad a los fines de la investigación, a actuar bajo identidad supuesta y a adquirir y transportar los objetos, efectos e instrumentos del delito y diferir la incautación de los*

mismos[84]".

Enseguida, el inciso 3º de la norma citada califica e identifica el uso de identidad supuesta con la técnica de agente encubierto, cuando señala que el agente encubierto deberá poner a disposición de la institución que haya dado su autorización la información que haya recabado.

Así, de lo previsto en los artículos 282 y 282 bis del cuerpo legal en estudio, tenemos que los requisitos generales de procedencia del agente encubierto en la investigación criminal española corresponderán a : (a) que se trate de fines de investigación policial, (b) investigaciones concernientes a la criminalidad organizada, (c) que se trate de alguno de los tipos penales expresamente contemplados en el párrafo 4 del artículo 282 bis, y (d) autorización judicial cuando pudieren verse afectados derechos fundamentales en el curso de la investigación.

A más de lo anterior, la ley regula algunos aspectos específicos sobre el ejercicio de la investigación mediante la técnica de agente encubierto. Con todo, según lo visto anteriormente, la legislación penal española y la chilena regula de manera muy similar la procedencia del agente encubierto, preceptuando que su empleo sea necesario para los fines de la investigación, que se trate de delitos cometidos mediante la forma de organización criminal, fijando ciertos tipos penales de especial gravedad para su procedencia, y la necesidad de autorización judicial en ciertos casos. Asimismo, el régimen de responsabilidad penal del agente encubierto, en ambos casos, es regido por el principio general de exención de responsabilidad del agente encubierto por las actuaciones realizadas en el contexto de la investigación.

Pese a estas similitudes sí existen algunas diferencias importantes en el ámbito de aplicación del agente encubierto en los países referidos. Primero, tratándose de los tipos penales especiales respecto de los que procede su uso en la legislación española, el catálogo de delitos y crímenes respecto de los que procede es más amplio en España, abarcando delitos como el tráfico de material nuclear, algunos delitos contra la salud pública, tráfico de ciertas especies de flora y de fauna, así como el delito de falsificación de moneda, entre otros.

Quizás la diferencia más relevante para efectos del presente dossier dice relación con lo

[84] Código procesal penal de España, artículo 282 bis. Actualizado al 29 de abril de 2021.

establecido en el inciso 2º del párrafo 6º del artículo 282 bis, que establece la modalidad del agente encubierto informático. Reza el tenor de la disposición, "*El agente encubierto informático, con autorización específica para ello, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos ilícitos*[85]". Como apunta Cánovas, la figura del agente encubierto virtual se introduce en el ordenamiento jurídico español mediante la reforma de la Ley Orgánica 13/2015, de 5 de octubre[86].

A pesar de que no se define lo que debe entenderse por agente encubierto informático, ciertamente es posible desprender de la norma que se tratará del uso de tecnologías de este tipo en el ejercicio de la técnica investigativa de agente encubierto. Estimamos que el tenor amplio en que se redacta la norma permite entender que se acepta de manera genérica el uso de las diversas tecnologías informáticas, como podrían ser no solo las operaciones hechas mediante un ordenador, si no que las efectuadas a través del empleo de algún *software*.

Pese a la falta de definición legal, se ha entendido que "*el agente encubierto informático es una especialidad dentro de los agentes encubiertos, un instrumento de investigación por el que un policía judicial puede actuar bajo una identidad fingida en comunicaciones a través de canales cerrados de comunicación con el fin de esclarecer alguno de los delitos cometidos en el seno de organizaciones criminales*[87]".

Ahora, la disposición del artículo 282 bis ha suscitado amplias consideraciones en cuanto al estudio del agente encubierto informático, especialmente en lo relativo a su procedencia. En este sentido, Cánovas ha detectado algunas de las problemáticas fundamentales en el desarrollo y aplicación del agente encubierto informático, identificando factores relativos a los requisitos legales de su aplicación, la afectación de derechos fundamentales en su uso, la inducción a la comisión de delitos en su empleo, así como el desarrollo de estrategias policiales que configuren un ilícito jurídico, entre otros factores[88].

En lo tocante a qué organismo se encuentra facultado para desarrollar este tipo de técnica

[85] Código procesal penal de España, artículo 282 bis, párrafo 6. Actualizado al 29 de abril de 2021.
[86] CÁNOVAS, Álex (2017). *Agente Encubierto Online*. Tesis de pregrado. Universitat Autònoma de Barcelona. p. 12.
[87] CLUSA, Alejandro (2019). *El Agente encubierto informático*. Tesis de fin de grado. Universidad de Zaragoza. p. 4.
[88] CÁNOVAS, Álex (2017). *Agente Encubierto Online*. Tesis de pregrado. Universitat Autònoma de Barcelona. pp. 13-23.

investigativa, tenemos que no pueden todas las fuerzas de seguridad ejercer las funciones del agente encubierto informático, si no que "*el ejercicio de la función de agente encubierto informático se encuentra reservado para los integrantes de la Policía Judicial quedando por tanto excluidos el resto de los miembros de las Fuerzas y Cuerpos de Seguridad del Estado*[89]", lo que viene a restringir su utilización.

Asimismo, y como bien señala Clusa, el ejercicio de este tipo de medio de investigación debe sujetarse a los principios rectores que establece la ley penal, correspondientes a los preceptuados por el artículo 588 bis a 1) LECrim, cual reza que "*durante la instrucción de las causas se podrá acordar alguna de las medidas de investigación reguladas en el presente capítulo siempre que medie autorización judicial dictada con plena sujeción a los principios de especialidad, idoneidad, excepcionalidad, necesidad y proporcionalidad de la medida*[90]", todo lo anterior tendiente a la protección de los derechos fundamentales que pueden verse afectados en el desarrollo de la investigación mediante el empleo de estos medios, según se hubo referido como problemática en el ámbito de aplicación del agente encubierto informático[91].

De manera general, se ha referido que la aplicación de estos medios investigativos está dada por límites generales, en tanto "*la medida debe ser idónea y útil para el fin pretendido, obtener pruebas del delito investigado y su duración no debe exceder más de lo necesario, puesto que se están vulnerando derechos fundamentales de la persona investigada. Este fin justifica su aplicación en el ámbito objetivo, subjetivo y la duración*[92]".

Entonces, cabe señalar que la consagración expresa del agente encubierto informático resulta desde la óptica investigativa como un acontecimiento deseable, ciertamente la incorporación de todo tipo de nueva tecnología debe realizarse en consonancia con el respeto de las garantías procesales de los intervinientes en el proceso penal.

Así, se les ha caracterizado como medios subsidiarios de investigación, en sentido que

[89] CLUSA, Alejandro (2019). *op. cit*. p. 7.
[90] Ley de Enjuiciamiento Criminal. España. Recurso electrónico disponible en el sitio online de la Agencia Estatal Boletín Oficial del Estado (España) https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036.
[91] CLUSA, Alejandro (2019). *op. cit*. pp. 21-24.
[92] PALOP. Melania (2017). *Protección jurídica de menores víctimas de violencia de género a través de internet*. Tesis Doctoral, dirigida por José Bonet Navarro, profesor de Derecho procesal. Universitat Jaume. p.191.

"*la excepcionalidad de la aplicación de las medidas de investigación tecnológica constituye un medio subsidiario de investigación debido a la vulneración de los derechos fundamentales ocasionados en las personas investigadas. Por tanto, su autorización en sede judicial no debe ser sistemática*[93]".

b. Argentina

El Código procesal penal de Argentina no emplea el concepto de agente encubierto. Sin perjuicio de ello, el artículo 296 emplea la técnica de los investigadores bajo reserva, disponiendo que "*El representante del Ministerio Público Fiscal podrá solicitar al juez en audiencia unilateral que se autorice la reserva de identidad de uno o varios investigadores si ello fuera manifiestamente útil para el desarrollo de la investigación. El juez fijará el plazo de la reserva de identidad que sólo será prorrogado si se renuevan los fundamentos de la petición*[94]".

A mayor abundamiento, fuera del Código Procesal Penal encontramos una ley especial, la Ley Nº 27.319, que regula la Investigación, Prevención y Lucha de los delitos complejos, regulando ciertas herramientas y facultades de investigación, rigiéndose por los principios jurídicos de necesidad, razonabilidad y proporcionalidad, conforme a su artículo primero[95].

El artículo 3º de la ley establece una definición legal del agente encubierto, refiriendo que "*Será considerado agente encubierto todo aquel funcionario de las fuerzas de seguridad autorizado, altamente calificado, que presta su consentimiento y ocultando su identidad, se infiltra o introduce en las organizaciones criminales o asociaciones delictivas, con el fin de identificar o detener a los autores, partícipes o encubridores, de impedir la consumación de un delito, o para reunir información y elementos de prueba necesarios para la investigación, con autorización judicial*[96]".

---

[93] PALOP, Melania (2017). *op. cit.* p. 192.

[94] Ministerio de Justicia y Derechos Humanos (2014). Código Procesal Penal de la Nación. Buenos Aires, Sistema Informático Argentino de Información Jurídica. 101 p. 82. Recurso electrónico disponible en http://www.saij.gob.ar/docs-f/codigo/Codigo_Procesal_Penal_de_la_Nacion.pdf.

[95] Ley Nº 27.319 (Argentina). Recurso electrónico disponible en el sitio online del gobierno argentino, http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268004/norma.html.

[96] Ibídem.

Enseguida, el artículo 2º establece taxativamente los tipos penales respecto de los cuales resulta procedente el uso del agente encubierto, refiriendo los delitos cometidos por asociaciones ilícitas, así como los relativos al tráfico de estupefacientes, entre otros, como algunos delitos aduaneros.

El articulado de la ley también establece la necesidad del uso del agente encubierto para el desarrollo de la investigación, así como el principio de la exención de responsabilidad para el agente encubierto en lo tocante a las actuaciones investigativas realizadas. De esta manera, su regulación sigue de cerca a lo preceptuado en la legislación chilena y española.

Una de las novedades que presenta la Ley Nº 27.319 dice relación con la consagración expresa de la figura del agente revelador en su artículo 5º, señalando que "*Será considerado agente revelador todo aquel agente de las fuerzas de seguridad o policiales designado a fin de simular interés y/o ejecutar el transporte, compra o consumo, para sí o para terceros de dinero, bienes, personas, servicios, armas, estupefacientes o sustancias psicotrópicas, o participar de cualquier otra actividad de un grupo criminal, con la finalidad de identificar a las personas implicadas en un delito, detenerlas, incautar los bienes, liberar a las víctimas o de recolectar material probatorio que sirva para el esclarecimiento de los hechos ilícitos*[97]".

Finalmente, no se establece de manera expresa en qué tipos de medios puede constituirse el ejercicio de la técnica de agente encubierto. Por ello, pese a no consagrar alguna figura como la del agente encubierto informático, o el uso de las tecnologías computacionales en su desarrollo, ciertamente pareciera ser que la ley no limita el empleo de ninguna tecnología.

[97] Ley Nº 27.319 (Argentina). Recurso electrónico disponible en el sitio online del gobierno argentino, http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268004/norma.html.

c. Otros países latinoamericanos

El Código Procesal Penal colombiano contempla la técnica investigativa del agente encubierto en su artículo 241, bajo el rótulo de análisis e infiltración de organización criminal. Dispone en este sentido que el fiscal "*ordenará la planificación, preparación y manejo de una operación, para que agente o agentes encubiertos la infiltren con el fin de obtener información útil a la investigación que se adelanta*[98]". Guardando similitud con otras legislaciones, la procedencia del agente encubierto como medio de investigación queda condicionado a la existencia de antecedentes fundados que permitan presumir que el imputado objeto de la investigación forma parte de una red criminal.

Enseguida, el artículo 242 del cuerpo legal en comento regula la actuación de los agentes encubiertos, supeditando su labor a que revista necesidad para el éxito de la investigación, así como la existencia de antecedentes fundados que permitan creer que el imputado continúa desarrollando la comisión de actividades criminales.

En este caso, la legislación procesal penal no incluye en la regulación del agente encubierto requisitos relacionados con la previsión de ciertos tipos penales que hayan de ser objeto de la investigación. Pareciera entonces que la aplicación de esta técnica de investigación se sujetará a los requisitos generales de que su uso sea indispensable para el éxito de la investigación, así como la existencia de actividad criminal organizada comprometida.

Tampoco se contempla la figura del agente encubierto informático. Sin embargo, se admite el uso de tecnologías informáticas en virtud de lo preceptuado en el artículo 244 del Código Procesal Penal colombiano, bajo el acápite de búsqueda selectiva en bases de datos, señalando que "*La policía judicial, en desarrollo de su actividad investigativa, podrá realizar las comparaciones de datos registradas en bases mecánicas, magnéticas u otras similares, siempre y cuando se trate del simple cotejo de informaciones de acceso público*[99]".

[98] Código procesal penal de Colombia. Recurso electrónico disponible en el sitio online de la Defensoría Penal de Colombia, https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_906_2004.pdf.
[99] Código procesal penal de Colombia. Recurso electrónico disponible en el sitio online de la Defensoría Penal de Colombia, https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_906_2004.pdf.

Sin embargo, pareciera ser que el uso de bases de datos encuentra un alcance más bien limitado, en tanto solo permite el cotejo de información de acceso público. Con todo, la regulación del agente encubierto no establece de manera expresa los medios de que esta técnica deba valerse, quedando abierta la discusión a si un agente encubierto de tipo informático podría o no ser admisible en el marco de la legislación vigente.

En el caso de Uruguay, tenemos que ni el Código de Proceso Penal ni el Código Penal establecen normas relacionadas con la técnica de investigación del agente encubierto[100]. Sin perjuicio de ello, la Ley N° 19.574, ley integral contra el lavado de activos, contempla en su artículo 64 la figura del agente encubierto en el contexto de este tipo de delitos. Dispone así que "*los Juzgados Letrados de Primera Instancia Especializados en Crimen Organizado podrán, mediante resolución fundada, autorizar a funcionarios públicos a actuar bajo identidad supuesta y a adquirir y transportar objetos, efectos e instrumentos de delito y diferir la incautación de los mismos*[101]".

En el caso de Uruguay también se establece la necesidad de que el delito investigado corresponda a aquellos ejecutados bajo la forma delictual del crimen organizado, así como la necesidad de que sea el juez con competencia criminal el que autorice su procedencia. Asimismo, pareciera ser que su ámbito de aplicación es más restringido que en otras legislaciones, en tanto no se señala un listado más amplio de tipos penales ante el que sea procedente, al estar inserto este instituto en una ley de carácter especial.

3.- Limitaciones de los *bots* y agentes encubiertos en la detección del ciberacoso

A la hora de considerar la implementación de *bots* como una herramienta para la detección del ciberacoso en redes sociales e Internet en general, uno de los problemas que puede provocar el uso de dichos *bots* se presenta en el contexto de que, al tratarse estos de inteligencia artificial y estar programados para detectar ciertas palabras que ayuden a captar cuándo se está en presencia de ciberacoso, este podría tener un índice de falibilidad si no cuentan con una

[100] Ver sitio online de IMPO, Centro de Información Oficial, Sección de Normativa y Avisos Legales del Uruguay, impo.com.uy.
[101] Ley N° 19.574, ley integral contra el lavado de activos (Uruguay). Disponible en sitio online de IMPO, Centro de Información Oficial, Sección de Normativa y Avisos Legales del Uruguay, impo.com.uy.

amplia base de datos, al no reconocer algunas agresiones verbales como insultos o amenazas, o directamente no ser capaz de detectar cuándo una imagen es empleada con fines de humillación.

Del mismo modo, así como las complicaciones técnicas, también hay que considerar aquellas de índole legal, puesto que un *bot*, si bien no es una persona humana, recaba información que posteriormente puede ser utilizada por estas, por lo que es necesario que exista un límite que fije su marco de acción.

i.- Dificultades lingüísticas por parte de los *bots* para la detección del ciberacoso

Ante la posibilidad de incorporar *bots* como herramienta para combatir situaciones de ciberacoso en las redes sociales, es necesario plantearse también las eventuales dificultades que esto puede traer aparejado para su correcta implementación y la obtención de un óptimo rendimiento, así como analizar posibles soluciones a estos casos.

En relación con los obstáculos que emanan de dificultades lingüísticas, el Instituto Milenio Fundamentos de los Datos se encuentra desarrollando una investigación para mejorar la información que circula por Internet, y especialmente las expresiones de odio en redes sociales, como por ejemplo en *Facebook* o en *Twitter*, que constituyen dos de las redes sociales más utilizadas en la actualidad, y que, desgraciadamente, en muchas ocasiones son empleadas con finalidades que contrarían la función para la cual fueron creadas y, dicho sea también, los términos y condiciones que estas redes sociales señalan para su correcto uso y que el usuario debe aceptar para formar parte de ellas, siendo así utilizado un lenguaje que contiene expresiones de odio o desprecio hacia terceros, o incluso amenazas que podrían ser reales y que es necesario detectar para poder efectuar las acusaciones pertinentes, apoyando por ello la necesidad de buscar herramientas automatizadas para detectar ese tipo de mensajes y conversaciones en las redes sociales; sin embargo, uno de los problemas que precisamente detecta Bárbara Poblete es respecto de los idiomas, ya que se necesita desarrollar herramientas que detecten estas expresiones de odio o de ciberacoso, pero en una mayor variedad de idiomas en los que existen menos herramientas.

No obstante lo señalado por la académica Bárbara Poblete, podemos observar que las limitaciones no solo están dadas por el idioma, que sin lugar a dudas es una barrera muy potente a la hora de implementar *bots* que detecten expresiones ofensivas, producto de la gran diversidad de culturas que transitan diariamente por el mundo y, por tanto, la gran variedad de idiomas que pueden emplear las personas incluso en un mismo territorio; sino que también es necesario contemplar la limitación en la capacidad de un *bot*. Esto es debido a que, cuando hacemos referencia a los *bots*, estamos hablando de *softwares* que simulan ser un humano, en ocasiones incluso capaz de mantener un diálogo con personas reales, como en el caso de los "*chatbots*", sin embargo, sea cual sea la finalidad para la que esta herramienta haya sido configurada, su actuación dependerá esencialmente de la tecnología que lo sustente y, por consecuente, de los avances de la propia tecnología.

Al contrario que los humanos, los cuales poseemos una inteligencia cognitiva, los *bots* tan solo tienen un conocimiento inducido en su programación y, por tanto, es mucho más restringido y específico. Si bien es cierto, como ya fuere mencionado con anterioridad, que a la hora de realizar una tarea repetitiva un *bot* podrá ser más rápido y eficiente que un humano, tampoco es menos cierto que este se encontrará mucho más limitado por el contexto ante ciertas situaciones en que varíe alguna condición frente a las cuales está configurado para actuar. Esta limitación, llevada al plano lingüístico, precisamente puede contemplarse ante el evento de que un *bot* sea configurado para la detección de determinados insultos o comentarios que puedan resultar ofensivos en las redes sociales, pero que, sin embargo, al tratarse de un medio informal, estos puedan ser empleados por los usuarios con una escritura alternativa para la comunicación del mismo contenido, ya sea mediante errores ortográficos -tanto intencionados para evitar que el *bot* detecte una determinada palabra, como aquellos que se cometan inintencionadamente-, o al cambio de ciertas letras por caracteres numéricos (por ejemplo, usuarios que cambian una letra "o" por el número "0", o la letra "i" por el número "1", con fines de autocensura), o incluso la omisión y sustitución por un asterisco (*) de alguna de las letras de la palabra para no hacer empleo explícito de esta, pero cuyo receptor es capaz de descifrarla y comprenderla sin mayor dificultad. Todo esto dependerá del ingenio y creatividad del emisor del mensaje, del mismo modo que la eficacia a la hora de evitar estas situaciones descritas dependerá de los conocimientos, esfuerzos y la misma creatividad por parte del programador de este *bot*.

Como un obstáculo adicional al actuar de los *bots*, encontramos las imágenes de contenido directamente ofensivo, y aquellas que se pueden utilizar como indirectas en determinado contexto, y que son de difícil detección por una herramienta en que no hay intervención humana directa. Entre estos últimos casos podemos destacar los llamados "*memes*", los cuales, de acuerdo con la definición de la RAE, consisten en una "*imagen, video o texto, por lo general distorsionado con fines caricaturescos, que se difunde principalmente a través de internet*[102]". Estos archivos con contenido multimedia circulan a través de Internet, especialmente al interior de las redes sociales como *Twitter*, *Instagram* o *Facebook*, y de servicios de mensajería instantánea como *Whatsapp* o *Telegram*, los cuales, acompañados generalmente con algún texto, tratan de representar de manera humorística una idea, concepto, o pensamiento con que el usuario al que llega esta imagen o video se identificará, y que puede caricaturizar desde un evento cotidiano hasta contingencias sociales o políticas. Por lo general, el usuario que lo crea o lo comparte públicamente tiene el objetivo de "viralizar" dicho contenido para provocar tanto risas como indignación en el receptor, entre otros sentimientos, según la temática en que se encuentre enfocada este meme.

Si bien estos memes pueden verse con una finalidad meramente de entretención, en ocasiones se envían con el fin de humillar o dar indirectas a quien lo recibe, especialmente cuando el agresor trata de crear uno personalizado y específicamente dedicado a la persona que desea menoscabar, incluso llegando a usar sus propias fotografías, para posteriormente compartirlo en algún grupo en común con la víctima, como podrían ser los chats de cursos escolares de *Whatsapp*, o grupos de *Facebook*, o su envío directamente por privado -y en ocasiones de manera anónima- a quien será la persona afectada, lo cual puede llegar a provocar daño o malestar en estas personas, especialmente en los más jóvenes.

Este tipo de situaciones constituyen una traba técnica a la potencial labor de un *bot* que trate de recopilar pruebas sobre situaciones de ciberacoso, toda vez que es difícil que dentro de la base de datos de estos se encuentre tal imagen o que pueda detectar el texto que incluye, así como la forma agresiva en que pueda estarse empleando una fotografía que en cualquier otro contexto podría no implicar mayor problema.

[102] Diccionario de la Real Academia Española: "Meme".

En este sentido, los *bots* poseen desventaja por sobre la labor de supervisión de un agente humano. Ambas limitaciones señaladas en los *bots* poseen un origen lingüístico. "*Las palabras se tratan como elementos carentes de significado y no se enfrentan a los grandes retos del procesamiento del lenguaje natural: la ambigüedad, la contextualización y la variabilidad lingüísticas. El lenguaje es ambiguo por naturaleza a todos los niveles en los que se estructura: morfológico, sintáctico, semántico, pragmático y discursivo. Y ofrece innumerables fórmulas de expresión que, por si fuera poco, dependen además del uso individual: único, personal, irregular y más veces de las que nos gustaría, imperfecto*[103]".

De esta forma, se evidencia que solo un *bot* programado con buenas capacidades de comprensión del lenguaje natural ("NLU" o "*Natural Language Understanding*") podría hacer frente a estos obstáculos de origen lingüístico, por lo que, para poder superar esta barrera, se hacen necesarios grandes esfuerzos por parte de los informáticos que desarrollan estas herramientas, así como que puedan contar con la tecnología más avanzada a su disposición.

ii.- Utilización de *bots* y agentes encubiertos para la detección del ciberacoso en niños menores de 14 años frente al derecho a la privacidad

Una segunda limitación que puede observarse dice relación con el derecho a la privacidad, puesto que, más allá de que el *bot* o un agente encubierto cibernético detecte una situación de ciberacoso, es relevante poder tomar acciones en contra de ellas, lo cual implica conocer la identidad del emisor de estos discursos de odio, insultos o amenazas, algo que no siempre es fácil, debido a que una de las características que reviste el ciberacoso consiste en la posibilidad de anonimato, por lo que sería necesario indagar desde qué computadora o teléfono celular fue enviado dicho contenido.

Por otro lado, en el caso de los niños menores de 14 años, para controlar mediante *bots* si estos son autores o víctimas de ciberacoso en edades tempranas, surge el conflicto de si dicha medida, al tratarse de una medida intrusiva, requeriría que los padres estuvieran en conocimiento de ello y autorizasen la aplicación de tal medida, puesto que, eventualmente, podría provocar

[103] Blog de Inbenta. *Chatbots: ¿buenos o malos imitadores de la interacción humana?* 08 de Mayo de 2019. [En línea] en https://www.inbenta.com/es/blog/chatbots-buenos-o-malos-imitadores-de-la-interaccion-humana/ [consulta: 25.09.2020].

que estemos en presencia de un caso de invasión a la privacidad de las personas, ya que pocos usuarios tienen en consideración a la hora de estar presentes en redes sociales que no solo comparten en ellas aquello que publican de forma explícita y consentida, sino que también entregan sin darse cuenta otros datos como la dirección IP ("*Internet protocol address*"), la cual consiste en "*la dirección inequívoca de un dispositivo en una red interna o externa*[104]" y que, como puede deducirse, constituye una información muy valiosa, puesto que con ella es posible identificar el dispositivo desde el cual se accedió a la red y, con ello, localizar por tanto al emisor de ciertos mensajes y publicaciones.

El tema de la implementación de *bots* o agentes encubiertos, aparte de abrir una ventana a una posible invasión a la privacidad mediante la localización de personas en la red, también podría implicar el eventual acceso a conversaciones o publicaciones privadas de los usuarios de alguna red social, lo cual pudiera ser necesario para hacer efectivo este cometido de detectar cuándo se está en presencia de contenido constitutivo de ciberacoso.

Este último punto es especialmente importante, sobre todo en el caso de los niños menores de 14 años, los cuales no pueden expresar su consentimiento válidamente para la aplicación de dichas medidas.

En el caso de estos menores, y como posible justificación a la aplicación de estas medidas intrusivas para evitar que estos sufran un daño por situaciones de ciberacoso, es relevante destacar el artículo 3.1 de la "*Convención sobre los Derechos del Niño*". Esta convención se aprueba como tratado internacional de derechos humanos el 20 de noviembre del año 1989, con el objetivo de reconocer a los niños como individuos con derecho de pleno desarrollo físico, mental y social, así como con derecho a expresar libremente sus opiniones. Del mismo modo, aspira a que los derechos de los niños contemplados en ella sean respetados por los Estados firmantes, toda vez que, si bien muchos poseen leyes internas que los protegen, no siempre son aplicadas.

A su respecto, el artículo 3.1 de dicha convención señala lo siguiente: "*En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar*

[104]Digital Guide IONOS. *Direcciones IP: Todo lo que debes saber.* 02 de septiembre de 2020. [En línea] en https://www.ionos.es/digitalguide/servidores/know-how/direccion-ip/ [consulta: 01.10.2020].

social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño[105]".

Adicionalmente, como instrumento internacional, también son destacables las "*Observaciones General del Comité de Derechos del Niño*", especialmente la Observación General Nº 14, denominada "*Sobre el derecho del niño a que su interés superior sea una consideración primordial*", en la cual se proclama a este interés superior del niño como "un derecho, un principio y una norma de procedimiento". A su respecto, esta observación no solo se remite a lo señalado por la Convención sobre los Derechos del Niño, sino que también añade que "*La plena aplicación del concepto de interés superior del niño exige adoptar un enfoque basado en los derechos, en el que colaboren todos los intervinientes, a fin de garantizar la integridad física, psicológica, moral y espiritual holísticas del niño y promover su dignidad humana*[106]".

Por otro lado, en normativas internacionales que regulan el tema, podemos destacar también nuevamente el "*Convenio de Budapest sobre la ciberdelincuencia*", puesto que dicho instrumento se encarga de otorgar la facultad a los Estados miembros para adoptar medidas que sean necesarias para la tipificación de aquellos delitos relacionados con la pornografía infantil, lo cual puede ser aplicable en el marco del presente trabajo, puesto que el ciberacoso incluye diversas formas donde puede incluirse la humillación mediante la publicación de contenido sexual del afectado.

Si bien ya analizamos previamente que esta convención no regula explícitamente el ciberacoso, tenemos en claridad que protege a los niños ante eventos mediante los cuales se vea vulnerada su dignidad a través del almacenamiento y publicación de pornografía infantil. De este modo -analizando el convenio en esta ocasión desde la perspectiva de una eventual vulneración a la privacidad de los niños con la aplicación de medidas intrusivas para evitar el ciberacoso- podría justificarse dicha vulneración, toda vez que la adopción de esta medida por

[105] Convención sobre los Derechos del Niño. 1989.
[106] Observaciones Generales del Comité de Derechos del Niño. Observación General Nº 14.

parte de los Estados tendría la finalidad de que los menores no sean expuestos indebidamente en la red mediante la publicación de contenido pornográfico que terceros pudieran solicitarle.

Así como el Convenio de Budapest protege a los niños en cuanto a ser víctimas de pornografía infantil y obliga a los Estados miembros a tomar medidas para combatirlo, justificándose entre ellas la intercepción de las comunicaciones judicialmente autorizada para la obtención de medios de prueba de la comisión de este delito -tal como incorporó la Ley Nº 19.927 en nuestro Código Penal en su artículo 369 ter, que combate la pedofilia-, también podría contemplarse la opción de que el interés superior del niño tenga prioridad por sobre la privacidad de estos en la red, con el fin de protegerlos del ciberacoso mediante el uso de *bots*, por lo que sería factible en el futuro que el empleo de *bots* encontrase cierto amparo en la legislación, tratando de hacerlo concordar en lo posible con el respeto del derecho a la privacidad, toda vez que la información recabada por estos solo pudiese ser utilizada con la finalidad de protegerlos de un mal mayor, como es el caso de recibir agresiones que puedan afectar su bienestar psicológico. De este modo, se requeriría una actualización de la normativa vigente, pero que parece estar en cierta armonía con la normativa internacional.

Todas estas normas internacionales analizadas son relevantes a la hora de considerar la aplicación de las medidas señaladas, puesto que disponen que los intereses del niño tienen máxima prioridad y deben constituir una consideración primordial en la toma de decisiones que les afectan, de modo que justificaría una actuación en la que pudiera considerarse una vulneración a la privacidad, de manera que esta quedaría amparada por la ley en busca de un bien mayor: el interés superior del niño.

En el caso del agente encubierto cibernético, el trato respecto a una vulneración del derecho a la privacidad es muy distinto, puesto que, en caso de que este se infiltrase en chats de servicios de mensajería instantánea o en grupos creados en redes sociales como un miembro más para poder recabar pruebas sobre ciberacoso entre los más jóvenes, este no estaría cometiendo realmente ninguna vulneración a la privacidad de los participantes del grupo, sino que cumpliría una función similar a la que efectúa el agente encubierto cuando actúa al interior de organizaciones criminales, encontrándose directamente involucrado en el lugar en que se está cometiendo el ilícito. Sin embargo, si fuese requerida la interceptación propiamente tal de

comunicaciones como podrían ser chats privados, sí estaríamos ante una posible vulneración, toda vez que la ley solo regula esta actuación del agente encubierto respecto a una lista taxativa de delitos, entre las que no se incluye el ciberacoso. Por tanto, del mismo modo que la ley ampara su actuación ante delitos relacionados a la pedofilia o al crimen organizado, se hace necesaria una regulación más amplia que pueda permitir válidamente su actuar en la red ante una mayor variedad de delitos.

CAPÍTULO III. VALOR PROBATORIO DE LA INFORMACIÓN RECABADA POR BOTS Y AGENTES ENCUBIERTOS COMO MEDIO DE PRUEBA

1. Consideraciones generales sobre la prueba

Aunque nuestro ordenamiento jurídico no define expresamente lo que debemos entender por el concepto de prueba, los tratadistas se han encargado de desarrollar abundantes reflexiones sobre esta materia, en virtud de las cuales podemos concluir que se trata de un concepto polisémico en el ámbito jurídico. Así, para Eduardo Couture "*en ciencia, probar es tanto la operación tendiente a hallar algo incierto, como la destinada a demostrar la verdad de algo que se afirma como cierto. En sentido jurídico, y específicamente en sentido jurídico procesal, la prueba es ambas cosas: un método de averiguación y un método de comprobación*[107]".

En un sentido similar se expresa Casarino, quien señala que el concepto de prueba puede referirse a la actividad de probatoria, a la convicción del tribunal, o a los resultados provenientes de la actividad desplegada por las partes; refiriendo en un sentido general que el concepto de prueba, o prueba judicial, corresponde a "*la demostración, por los medios que la ley establece, de la verdad de un hecho que ha sido controvertido y que es fundamento del derecho que se pretende* (…). *Es por eso que también se define la prueba como un medio de controlar las proposiciones que los litigantes formulan en juicio*[108]". Cabe destacar en esta conceptualización una nota de distinción, correspondiente al rol de la ley ante los medios de prueba: que la prueba se produce mediante los medios que la ley establece.

De todo lo anterior podemos colegir cuál es la función que cumple la prueba en el sistema procesal, cual corresponde a la acreditación de los hechos ante el tribunal, para generar su convicción y obtener en juicio. Es por ello que en la doctrina procesalista se ha barajado el concepto de verdad como la entidad que se busca comprobar en el proceso.

---

[107] COUTURE, E. (1958). *Fundamentos del Derecho Procesal Civil.* 4° ed. Buenos Aires, Editorial Metropolitana. 2014, p. 217.

[108] CASARINO, M. (1911). *Manual de Derecho Procesal*. Derecho Procesal Civil. Tomo IV. Santiago, Editorial Jurídica de Chile. 2009, p. 45.

En este sentido Michelle Taruffo, analizando el rol del concepto de verdad, explica que "*el problema de definir la función de la prueba se conecta directamente con los diversos conceptos* de *proceso y de los objetivos del proceso judicial. Este problema se puede resolver adoptando teorías conforme a las cuales establecer la verdad de los hechos sea uno de los principales objetivos del proceso judicial*[109]".

Con todo, determinar cuál es la función de la prueba es solo una de las problemáticas que se erigen en el centro de la teoría de la prueba. Como señalara Casarino, "*la teoría general de la prueba considera que son elementos de ella: el objeto sobre el cual debe recaer; los sujetos o las personas que deben proporcionarla; los medios de que se vale el sujeto para probar; y, por último, su eficacia, esto es, lo que la prueba vale en definitiva*[110]".

En la materia que nos ocupa, los hechos ocurren a través de las redes informáticas y de telecomunicaciones, que son altamente volátiles y pueden ser cometidos desde distintos lugares, incluso desde localidades distintas respecto de aquellas en que se encuentra la víctima, lo que tensiona tanto al sistema procesal como al aparato persecutorio penal.

En lo siguiente nos abocaremos a analizar estas problemáticas, centrándonos primero en el análisis de los medios probatorios y la eficacia de los medios de prueba y su eventual aplicación a los *bots*.

2. Procedencia de medios probatorios en el proceso chileno

Como decíamos, en el ámbito de todo sistema probatorio existen diversas cuestiones que lo estructuran y erigen su desarrollo. Así, dentro de las cuestiones fundamentales en la teoría de la prueba encontramos los tópicos de la procedencia de los medios de prueba, así como el correspondiente al estudio de los sistemas de valoración probatoria y la eficacia de la prueba. El primero de estos temas nos permite dilucidar qué medios probatorios podemos emplear en el

[109] TARUFFO, M. (2008). *La prueba*. Madrid, Marcial Pons. p. 20.
[110] CASARINO, M. (1911). *op cit.* p. 46.

proceso para acreditar determinadas circunstancias fácticas, mientras que el segundo nos dirige a determinar el valor probatorio que una probanza específica presentará en juicio.

De manera análoga a la ausencia de una definición legal del concepto de prueba, nuestra ley tampoco contempla una definición de medio probatorio, pero se ha referido que "*se entiende por medio de prueba el instrumento, la cosa o la circunstancia en los cuales el juez encuentra los motivos de su convicción frente a las proposiciones de las partes*[111]".

En cuanto a la procedencia de un medio probatorio existen distintas normas legales según la naturaleza del proceso en cuestión. Así, corresponde diferenciar las normas vigentes en el Código de Procedimiento Civil, tratándose de los procesos de esta naturaleza, así como las normas del Código Procesal Penal, al tratarse de materias penales. Asimismo, existen normas especiales en otros procesos, como lo es el caso del proceso laboral regulando en el Código del Trabajo.

En cuanto al procedimiento civil, el código del ramo no parece regular expresamente cuáles son los medios de prueba que deberán considerarse como procedentes, en tanto los artículos 318 y siguientes del Código de Procedimiento Civil, correspondientes al Título IX que regula la prueba en general, se encargan de reglamentar la fase de prueba, sin establecer disposiciones generales sobre los medios probatorios.

Así, es el artículo 341 del Código de Procedimiento Civil el que enumera los medios de prueba en particular, correspondiendo estos a los instrumentos, los testigos, la confesión de parte, la inspección personal del tribunal, el informe de peritos y las presunciones judiciales. Asimismo, este ámbito se ve extendido hasta el campo de los documentos electrónicos, en tanto el artículo 3° de la Ley N° 19.799 establece el principio de equivalencia funcional entre el soporte electrónico y el soporte en papel, admitiéndose expresamente su admisibilidad en el artículo 5° del mismo cuerpo legal.

Sobre este particular, el profesor Casarino sostiene que no son procedentes más medios probatorios que los referidos por la ley, en tanto "*dentro de nuestro derecho positivo, la ley se ha encargado de enumerar, en forma taxativa, los medios probatorios con el objeto de evitar*

[111] CASARINO, M. (1911). *op cit*. p. 45.

que esta importante materia quede entregada al arbitrio del juzgador[112]", comentando sobre el artículo 341 recién citado, que "*se estima que estas enumeraciones son taxativas, o sea, que no existen otros medios probatorios para demostrar la verdad o falsedad de un hecho en juicio que los antes señalados*[113]".

Tratándose del proceso penal sí existen normas expresas que permiten determinar con mayor claridad el sistema de admisibilidad probatoria. En primer lugar, tenemos que el artículo 295 del Código Procesal Penal establece la libertad probatoria, refiriendo que "*Todos los hechos y circunstancias pertinentes para la adecuada solución del caso sometido a enjuiciamiento podrán ser probados por cualquier medio producido e incorporado en conformidad a la ley"*, norma de la cual puede colegirse que existe un criterio amplio de admisibilidad de medios probatorios.

Circunstancia anterior que se ve reforzada por la regulación de los medios particulares de prueba en el proceso penal, toda vez que se regulan expresamente la prueba de testigos, el informe de peritos y la prueba documental, pero consagrándose también una norma de clausura, correspondiente al artículo 323 del Código Procesal Penal, cual dispone que "*Podrán admitirse como pruebas películas cinematográficas, fotografías, fonografías, videograbaciones y otros sistemas de reproducción de la imagen o del sonido, versiones taquigráficas y, en general, cualquier medio apto para producir fe*", de manera que el legislador prevé expresamente el empleo de ciertas tecnologías como medios de prueba, estableciendo una permisibilidad extensa con tal que se trate de medios aptos para producir fe. Incluso se ha fallado por la Corte de Apelaciones de San Miguel, en la causa Rol 2605-2016, la procedencia de medios fotográficos pese a alegarse su exclusión por la prohibición del artículo 334 del Código Procesal Penal, respecto a la lectura de registros y documentos.

De esta manera, Sabas Chahuán ha entendido que las limitaciones a la admisibilidad probatoria dirán relación no con la procedencia de los distintos medios probatorios propiamente, sino con la ilicitud de la prueba, y también con la existencia de prohibiciones específicas, como en el caso del artículo 334 del Código Procesal Penal[114].

[112] CASARINO, M. (1911). *op cit*. p.45.
[113] Ibídem.
[114] CHAHUÁN, S. (2002). *Manual del nuevo procedimiento penal*. 2° edición. Santiago, Lexis Nexis. p. 306.

Finalmente, parece también pertinente revisar de manera sucinta las normas procesales del Libro V del Código del Trabajo, en consideración de la relevancia socio-jurídica que tiene la prohibición del acoso en las relaciones laborales, según se establece ya en el artículo 2° del mentado código. En este sentido, es su artículo 454 el que regula actividad probatoria en el procedimiento de aplicación general, en el contexto de la audiencia de juicio, regulando expresamente la admisibilidad y rendición de la prueba testimonial, documental, confesional y pericial.

Enseguida, este ámbito se ve extendido por lo referido en el párrafo tercero del numeral 1° del artículo 454, en tanto al establecer el orden de rendición de los distintos medios de prueba se refiere a la procedencia de "*los otros medios ofrecidos*", sin establecer un catálogo taxativo de los medios que podrán ser rendidos en juicio. A continuación, el numeral 8° del mismo artículo referido establece que "*Cuando se rinda prueba que no esté expresamente regulada en la ley, el tribunal determinará la forma de su incorporación al juicio, adecuándola, en lo posible, al medio de prueba más análogo*", estableciéndose un ámbito de admisibilidad probatoria muy amplio, de manera similar al principio de libertad de prueba del Código Procesal Penal.

En este sentido, la autora Marcela Díaz, desde la óptica que le compete en su calidad de jueza, ha referido respecto del tipo de prueba ofrecida en el proceso laboral que "*las partes podrán valerse de todo medio probatorio que estimen conveniente, con la finalidad de acreditar sus alegaciones, es decir, no existe límite probatorio*[115]", agregando que "*las partes se encuentran facultadas para valerse de todos los medios probatorios con que cuenten, para acreditar los puntos de prueba decretados por el tribunal, debiendo proporcionar los soportes electrónicos u otros medios idóneos para su incorporación en audiencia*[116]", de manera que el único condicionamiento en este ámbito de libertad probatoria dirá relación con la carga procesal de contar con los medios para incorporar la prueba en el proceso.

[115] DÍAZ, M. (2017). *Manual de procedimiento del trabajo.* Santiago, Librotecnia. p. 125.
[116] Ibídem. p. 134.

3. Valoración de la prueba en el sistema chileno

Según plantea Couture: "*El tema de la valoración de la prueba busca una respuesta para la pregunta: ¿qué eficacia tienen los diversos medios de prueba establecidos en el derecho positivo? Ya no se trata de saber qué es en sí misma la prueba, ni sobre qué debe recaer, ni por quién o cómo debe ser producida. Se trata de señalar, con la mayor exactitud posible, cómo gravitan y qué influencia ejercen los diversos medios de prueba, sobre la decisión que el magistrado debe expedir*[117]".

Analizando también el concepto de valoración de la prueba, los autores Horvitz y López lo conceptúan desde la óptica del proceso penal, definiéndola como "*el análisis crítico que hace el tribunal de las pruebas rendidas durante el juicio oral, con el objeto de decidir si se ha verificado o no las afirmaciones en las cuales se basan la acusación y la defensa, y adoptar la decisión de absolución o condena*[118]".

Tratándose del procedimiento civil, Casarino ha distinguido tres sistemas probatorios en cuanto a la valoración de la eficacia de los medios de prueba, correspondientes al sistema de prueba legal, la prueba libre o moral y el sistema de la sana crítica. En cuanto al primero, "*se caracteriza porque el legislador enumera taxativamente los medios probatorios que las partes pueden utilizar en juicio y señala, al mismo tiempo, al juez la eficacia probatoria que cada medio probatorio posee en particular*[119]", en concordancia con la postura del autor, para quien el artículo 341 del Código de Procedimiento Civil establece un catálogo taxativo de medios probatorios. Uno de los ejemplos más claros en esta materia está dado por el artículo 384 del mismo cuerpo legal, que enuncia detalladamente las reglas necesarias para valorar la prueba testimonial.

En cuanto al sistema de prueba libre o moral, el mismo autor refiere que "*se caracteriza porque el legislador no fija los medios probatorios, las partes acreditarán los hechos en la forma que mejor les acomode y el juez en su sentencia, por consiguiente, no está atado a regla alguna en cuanto a la valorización o ponderación de la prueba*[120]".

---

[117] COUTURE, E. (1958). *op cit.* p. 257.
[118] HORVITZ, M.y LÓPEZ, J. (2004) *Derecho Procesal Penal Chileno*. Tomo II. Santiago. Editorial Jurídica de Chile. p. 144
[119] CASARINO, M. (1911). *op. cit*. p. 48.
[120] Ibídem.

Finalmente, en cuanto al sistema de la sana crítica, Couture ha referido que "l*as reglas de la sana crítica son, ante todo, las reglas del correcto entendimiento humano. En ellas interfieren las reglas de la lógica, con las reglas de la experiencia del juez*[121]", a las que modernamente se han agregado las consideraciones pertinentes al conocimiento científicamente afianzado, respecto del cual se ha referido que "*cumple la función de garantía, conector o enlace de un enunciado fáctico desconocido a otro conocido*[122]".

Tenemos a este respecto que el Código de Procedimiento Civil establece mayormente un sistema de prueba legal o tasada. Sin embargo, algunas normas de dicho cuerpo legal han consagrado expresamente la procedencia del sistema de valoración de la sana crítica. Es el caso de la eficacia del informe de perito, en tanto el artículo 425 del Código de Procedimiento Civil establece que "*los tribunales apreciarán la fuerza probatoria del dictamen de peritos en conformidad a las reglas de la sana crítica*". Asimismo, tenemos el caso del artículo 429 del mismo cuerpo legal que, en el contexto de la invalidación de una escritura pública mediante la prueba testimonial, refiere en su inciso segundo que "E*sta prueba, sin embargo, queda sujeta a la calificación del tribunal, quien la apreciará según las reglas de la sana crítica*".

Tratándose del proceso penal, la norma pertinente corresponde al artículo 297 del Código Procesal Penal, que establece la valoración de la prueba, disponiendo que "*los tribunales apreciarán la prueba con libertad, pero no podrán contradecir los principios de la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados*".

Sobre este sistema de valoración de la prueba, Chahuán ha referido que "*el sistema que se consagra es el de la "libre valoración de la prueba" cuya esencia consiste en que el juez no se encuentra vinculado a reglas probatorias, es decir a disposiciones legales acerca de la eficacia de las pruebas*[123]".

En un sentido similar, los autores Horvitz y López refieren que el Código Procesal Penal chileno establece el sistema de libre convicción o sana crítica racional, definiendo este sistema de valoración como "*aquel caracterizado por la ausencia de reglas tendientes a regular el valor*

[121] COUTURE, E. (1958). *op. cit.* p. 70.
[122] CARBONELL, F. (2018). *Sana crítica y razonamiento judicial*. En BENFELD, Johann y LARROUCAU, Jorge (ed.), *La sana crítica bajo sospecha* (pp. 35-47). Valparaíso, Ediciones Universitarias de Valparaíso.
[123] CHAHUÁN, S. (2002). o*p. cit.* p. 309.

probatorio que el juez debe asignar a los medios de prueba, pero que impone al juez la obligación de fundamentar su decisión haciendo explícitas las razones que la han motivado[124]".

En otros procesos especiales se ha establecido el sistema de la sana crítica. Es el caso del artículo 465 del Código del Trabajo, que en el marco del proceso de aplicación general refiere que "*El tribunal apreciará la prueba conforme a las reglas de la sana crítica*". Es también el caso de la Ley Nº 19.968 que crea los Tribunales de Familia, cuyo artículo 32 reza "*los jueces apreciarán la prueba de acuerdo a las reglas de la sana crítica. En consecuencia, no podrán contradecir los principios de la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados*". En ambos casos, los jueces quedan sujetos al deber de fundamentar su sentencia y no contradecir los principios de la lógica, las máximas de la experiencia y los conocimientos científicamente afianzados.

4. Los *bots* como medio de prueba ante el sistema probatorio chileno

La interrogante por discernir implica determinar primeramente si los *bots* pueden entenderse como medios probatorios procedentes de emplearse en el proceso y, enseguida, cuál es el valor probatorio que les corresponde para el caso de que optemos por la respuesta afirmativa.

El meollo del asunto ha sido planteado antes por Couture, resultando plenamente aplicable a nuestra materia:

"*Los* textos *legales enumeran habitualmente los medios de prueba: instrumentos, testigos, confesión, juramento, inspección judicial, dictamen pericial y presunciones.*

El problema consiste en saber si esas pruebas pueden ser ampliadas con otras que no han sido objeto de previsión especial, pero que, respondiendo a conquistas de la ciencia, brindan día a día nuevas posibilidades de investigación frente a los hechos controvertidos[125]".

En efecto, determinar la procedencia de los *bots* como fuente de prueba implica analizar en su conjunto la procedencia de las tecnologías no previstas expresamente en la ley como medio

[124] HORVITZ, M. y LÓPEZ, J. (2004) o*p. cit.* p. 150
[125] COUTURE, E. (1958). *op. cit.*. p. 261.

de prueba. Así, establecer la procedencia de este mecanismo es un análisis que habrá de aportar no solo en esta materia específica, sino que también respecto de la procedencia de otras tecnologías en otras materias.

En este mismo sentido, Taruffo ha planteado la problemática de la procedencia de los medios informáticos como parte del procedimiento probatorio. Analizando el valor de la prueba informática refiere que "*surge el problema de establecer cuándo son admisibles estos muy peculiares datos y documentos como pruebas judiciales, como se pueden reunir presentar, y qué valor probatorio pueden alcanzar*[126]".

Contestar la primera interrogante, sobre la procedencia de los instrumentos informáticos como medio probatorio, en el caso de los *bots* implicará distinguir los distintos tipos de procesos que contempla nuestra legislación. Diferenciaremos entonces entre el proceso civil, el proceso penal y otros procesos especiales.

Tratándose del proceso civil, parece difícil admitir su procedencia como medio probatorio. Esto por cuanto, según se refirió anteriormente, de conformidad al artículo 341 del Código de Procedimiento Civil los medios probatorios que contemplan los procesos civiles corresponden a los instrumentos, los testigos, la confesión de parte, la inspección personal del tribunal, el informe de peritos y las presunciones judiciales; sin incluirse en caso alguno algún medio que permita entender que las tecnologías informáticas se han de considerar como medios probatorios procedentes y admisibles

Con todo, es posible considerar que el producto de la actuación de los *bots* sí podría ser empleada como medio probatorio en los procesos civiles. Lo anterior por cuanto la fuente de una probanza y el medio probatorio en sí mismo son diversos. Así, el resultado de las labores que sean arrojados por el empleo tecnológico de los *bots* podrá adquirir diversas formas, esperándose razonablemente que esta forma pueda corresponder a un documento que dé cuenta por escrito de los resultados en cuestión. De esta manera, la emisión de un documento electrónico que contenga un informe sobre las conclusiones arrojadas en el trabajo informático podrá incorporarse al proceso conforme a las reglas del artículo 348 bis. del Código de

[126] TARUFFO. M. (2008). *op. cit.* p. 85.

Procedimiento Civil y tener el valor probatorio correspondiente según la ley Nº 19.799 sobre documentos electrónicos.

Enseguida, creemos que la presentación de los *bots* como medio de prueba también puede verificarse de manera mediata mediante el informe de peritos. Este informe podrá contener un resumen del trabajo efectuado, de manera análoga a lo recién analizado, pero, además, podría extenderse a la explicación sobre el desarrollo y obtención de las conclusiones obtenidas, o la explicación del proceso informático en sí mismo. Todo lo cual facilitaría la incorporación de los *bots* al proceso civil, aunque sea indirectamente.

Lo anterior es particularmente relevante, pues la presentación de un medio de prueba no admitido por ley llevará a rechazar las probanzas vertidas en el proceso, teniendo por resultado la falta de acreditación de un hecho particular. Aún más, la Excma. Corte Suprema ha entendido que se entienden vulneradas las leyes reguladoras de la prueba cuando "*los sentenciadores invierten el onus probandi o carga de la prueba, rechazan las pruebas que la ley admite, aceptan las que la ley rechaza*[127]", entre otros casos. Y, aunque el artículo 341 del Código de Procedimiento Civil no rechaza ningún medio probatorio, en tanto establece positivamente un catálogo de medios procedentes, la interpretación de dicha disposición como una norma de carácter taxativo nos lleva a considerar *a contrario sensu* que los medios probatorios no admitidos expresamente por esta disposición deberán entenderse excluidos. Lo anterior, con la consecuencia de hacer procedente un recurso de casación en el fondo.

Pese a lo anterior, la improcedencia de los *bots* como medio de prueba en el proceso civil no resulta mayormente relevante en su rol como medio probatorio. Lo anterior por cuanto los *bots* no parecen estar funcionalmente concebidos para dar cuenta de la clase de hechos que se ventilan en un proceso civil. En este sentido, el Código Civil y el Código de Procedimiento Civil regulan de manera estricta la prueba de las obligaciones, de manera que la ley contempla los medios específicos de que deberán valerse los sujetos para probar las obligaciones, sin que el tráfico jurídico dé cuenta del empleo de los *bots* en estas materias. Ello especialmente si consideramos que el acoso como sustrato fáctico no habrá de tramitarse en los procesos civiles, sino que, en otros procesos como el proceso penal, el de familia y el de trabajo. Finalmente,

[127] Corte Suprema. Tercera Sala (Constitucional). Rol Nº 3075-2005. Santiago, Chile.

según se dijo, pese a no ser posible incluir directamente los *bots* como medio probatorio, si parece factible encuadrar el resultado de su trabajo en otras probanzas legalmente admitidas.

En cambio, tratándose del proceso penal, estimamos que la procedencia de los *bots* como medio probatorio debe ser aceptada plenamente. Ello por cuanto el Código Procesal Penal establece el principio de libertad probatoria y, aunque regula algunos medios de prueba de manera específica, ciertamente la ley establece que el tribunal podrá asimilar el medio de prueba no contemplado en la ley al medio de prueba más análogo que sí cuente con la recepción legal.

Por ello, y según dijimos anteriormente, estimamos que en el caso del proceso penal el único requisito que establece la ley será el cumplimiento de una carga procesal específica, que corresponde a la necesidad jurídica de proporcionar los medios tecnológicos que permitan incorporar el medio probatorio no contemplado en la ley al proceso, lo que, en la práctica, implicará facilitar los medios tecnológicos necesarios para que el juzgador pueda percibir la prueba aportada (ordenadores, discos, *softwares*, etc.).

Enseguida, admitida la procedencia de los *bots* como medio de prueba, es necesario determinar cuál podría ser el valor probatorio de estos. Sin embargo, como el Código Procesal Penal no regula el valor probatorio de las probanzas, a diferencia de lo que pasa en el proceso civil, será menester determinar primeramente cuál será el medio probatorio típico al que habrá de analogarse este medio de prueba informático.

Frente a tal interrogante, estimamos que debemos distinguir entre los *bots* como herramientas de pesquisa de hechos, respecto de los productos que se obtengan de su operación, esto es, los archivos informáticos que contengan evidencias. Teniendo en cuenta lo anterior, habremos de concluir que su operación requerirá del informe de peritos, entendido como la "*presentación al juicio de un dictamen u opinión sobre hechos controvertidos en él, para cuya adecuada apreciación se requieren conocimientos especiales de alguna ciencia o arte*[128]", mientras que el perito corresponde a "*toda persona que tiene conocimientos especiales sobre una materia determinada y apta, en consecuencia, para dar su opinión autorizada sobre un hecho o circunstancia contenido en el dominio de su competencia*[129]". Esto se entiende porque los *bots* tienen una naturaleza informática. En efecto, y según se hubo referido anteriormente,

[128] CASARINO, M. (1911) *op. cit*. p. 111.
[129] Ibídem. p. 111.

los *bots* corresponden a una especie de *software*, esto es, un instrumento propio de las ciencias informáticas, que requieren de conocimientos especializados en dicha disciplina para analizar los productos que se obtengan de su operación.

En vista de lo anterior, es importante considerar la regulación que el Código Procesal Penal establece sobre el informe de peritos, debiendo abordarse los presupuestos para su procedencia, los requisitos de su admisibilidad y el contenido del informe.

En cuanto a su procedencia, tenemos que, conforme al artículo 314 del Código Procesal Penal, "*los informes deberán emitirse con imparcialidad, ateniéndose a los principios de la ciencia o reglas del arte u oficio que profesare el perito*", norma que reafirma la naturaleza de este medio probatorio en cuanto a la especialidad de los conocimientos necesarios para su adecuada emisión.

En cuanto a la legitimación para solicitar que se decrete el informe de peritos como probanza en el proceso, la misma norma citada refiere que este puede ser solicitado por el Ministerio Público o por cualquier interviniente, lo que incluirá en estos casos al querellante o víctima que se haya visto afectado por los hechos constitutivos de acoso y que hayan sido investigados mediante estos medios tecnológicos.

Finalmente, tenemos que la procedencia del informe de peritos queda determinada por la concurrencia de los casos en que la ley admite el informe de peritos y por la necesidad de su emisión atendida la importancia de los hechos que motivan su solicitud. En cuanto a lo primero, el Código Procesal Penal no entrega una respuesta, sino que únicamente enuncia que debe estar prevista por la ley su procedencia.

Aunque es discutible la remisión al Código de Procedimiento Civil ante la exigencia de su previsión en la ley, por no haber una norma expresa que establezca la supletoriedad de las normas de su Libro II en materias penales, puede ser útil considerar los artículos 409 y 411 de este cuerpo legal. El primero señala de manera genérica que "*Se oirá informe de peritos en todos aquellos casos en que la ley así lo disponga, ya sea que se valga de estas expresiones o de otras que indiquen la necesidad de consultar opiniones periciales*". En este caso, se trata de una remisión genérica al establecimiento legal expreso de la necesidad de emplearse este medio probatorio. De esta manera, los casos en que será procedente el informe de peritos por el

mandato de esta norma serán más bien específicos, conllevando la dificultad que implica el que la ley contemple situaciones fácticas específicas.

Enseguida, el artículo 411 establece dos causales que harán procedente el informe de peritos, una genérica y otra especial. En este caso es la primera la que resulta relevante a efectos del tema en estudio, en tanto establece que "*Podrá también oírse el informe de peritos: 1°. Sobre puntos de hecho para cuya apreciación se necesiten conocimientos especiales de alguna ciencia o arte*". De esta manera, aunque la ley no especifique la necesidad de que se rinda informe de peritos cada vez que se empleen medios informáticos como medio de prueba, ciertamente la presentación de los *bots* como medio probatorio reúne la cualidad de necesitar la interpretación o explicación de un conocimiento especializado y que dé cuenta de su veracidad y significado.

Tratándose de la admisibilidad de estos instrumentos informáticos como medios probatorios, tenemos que el artículo 316 del Código Procesal Penal establece que "*El juez de garantía admitirá los informes y citará a los peritos cuando, además de los requisitos generales para la admisibilidad de las solicitudes de prueba, considerare que los peritos y sus informes otorgan suficientes garantías de seriedad y profesionalismo*".

En efecto, este ámbito de admisibilidad implica la necesidad de cumplirse con un estándar de objetividad e imparcialidad, en tanto "*cuando el perito actúa conforme con los criterios válidos y vigentes en la disciplina que se trate y los aporta al tribunal diciendo la verdad, se garantiza el mínimo necesario de imparcialidad científica, objetiva, que debe concurrir en el trabajo de examen y emisión del dictamen pericial*[130]", de manera que la admisibilidad de este medio probatorio tendrá la doble exigencia de ser emitido con veracidad, por un lado, pero también guardando la objetividad que es propia de las disciplinas científicas.

Es por ello que, pese a no ser procedente la inhabilitación de los peritos en el proceso penal, el artículo 318 del código del ramo establece que "*durante la audiencia del juicio oral podrán dirigírseles preguntas orientadas a determinar su imparcialidad e idoneidad, así como el rigor técnico o científico de sus conclusiones. Las partes o el tribunal podrán requerir al perito información acerca de su remuneración y la adecuación de ésta a los montos usuales para el tipo de trabajo realizado*", por cuanto un perito no podrá ser inhabilitado mientras

[130] AGUIRREZÁBAL, M. (2011). *La imparcialidad del dictamen pericial como elemento del debido proceso*. Revista chilena de derecho, 38(2), 371-378.

cumpla con requisitos básico de idoneidad en cuanto a su formación, pero sí en caso de no ejercerla debidamente al momento de declarar o emitir el informe correspondiente.

A continuación, el Código Procesal Penal regula también el contenido del informe de peritos en su artículo 315. Se establece a este respecto como contenido: "*a) La descripción de la persona o cosa que fuere objeto de él, del estado y modo en que se hallare; b) La relación circunstanciada de todas las operaciones practicadas y su resultado, y c) Las conclusiones que, en vista de tales datos, formularen los peritos conforme a los principios de su ciencia o reglas de su arte u oficio*".

La exigencia de describir la cosa o persona que fuere objeto de él permitirá informar al tribunal sobre la naturaleza y cualidades del medio empleado. Tratándose de los *bots*, será menester referir la naturaleza informática del medio empleado, así como la descripción de su especie como *software* y la función que está llamado a cumplir.

La segunda exigencia, la relación circunstanciada de las operaciones realizadas, podría resultar el punto más complejo de la presentación de este medio probatorio. Lo anterior por cuanto la descripción de las operaciones realizadas necesariamente habrá de dar cuenta de un fenómeno técnico en vista de su naturaleza, de manera que en esta parte se apreciará con mayor claridad el objeto del informe de peritos.

La tercera exigencia, referente a las conclusiones a las que arribare en virtud del informe, es quizás la más relevante en lo tocante a este medio probatorio. Ello por cuanto, tras la descripción del objeto analizado y de las operaciones efectuadas, el juez de la causa no necesariamente va a arribar a conclusiones propias en vista de la tecnicidad de la disciplina informática. Por ello, es justamente la conclusión a la que arribe el perito respecto de las operaciones realizadas por los *bots* la que permitirá al tribunal formarse la convicción sobre la acreditación de los hechos alegados.

En este caso particular, las conclusiones que serán necesarias para formar debidamente la convicción del tribunal en los casos de ciberacoso dirán relación con la acreditación de que efectivamente se hubo verificado los hechos constitutivos de dichas conductas, todo mediante la actuación del sistema informático y la información detectada. Finalmente, tenemos que el valor probatorio que en definitiva presente este medio probatorio será determinado por el juez, según el análisis de toda la prueba rendida y la efectiva acreditación de los hechos alegados.

Corresponderá al juez determinar si este medio informático será suficiente por sí solo para dar cuenta de los ilícitos investigados mediante su aportación a través del informe de peritos o si, además, estimará necesaria la concurrencia de otros medios probatorios conjuntamente.

Por todo lo anterior, cobrará también relevancia, como se ha dicho, la cadena de custodia a que deberá someterse este tipo de probanzas, en vista de su especialidad, y considerando especialmente que "*la cadena de custodia trata de asegurar que la prueba que se ha recogido durante la fase de instrucción sea la misma que se presenta ante el juicio oral y que por tanto mantenga la fidelidad y evitar así que se manipule o se transforme*[131]", en consideración de los medios de modificación que pueden intervenir en la manipulación de estos medios de investigación durante el transcurso del proceso, todo lo cual supone un desafío adicional a los operadores del sistema judicial y criminal en aras a conservar la fidelidad de las pruebas producidas.

5. La prueba informática en el derecho comparado e internacional

Desde un ámbito conceptual, cabe referir que las tecnologías informáticas y electrónicas han dado lugar a una variada gama de medios probatorios modernos. Así, se ha referido que "*una prueba electrónica es toda información con valor probatorio incluida o transmitida por un medio electrónico. Concretamente, podemos diferenciar entre datos almacenados en sistemas informáticos y datos transmitidos a través de redes de comunicación informática*[132]".

Como se hubo referido anteriormente, en los sistemas jurídicos comparados e internacionales existen distintas normas o tratados que buscan establecer una regulación del desarrollo de la ciencia informática en su conjunto. Sin embargo, no parece existir una regulación estrictamente abocada a la regulación de los *bots*, de manera que el desarrollo de la materia a nivel legislativo resulta ser más bien escaso.

Tratándose de Sudamérica, existen diversos estudios sobre la necesidad de implementar una regulación específica sobre la materia. Así, en el caso ecuatoriano, la autora Gladys Proaño

[131] CÁNOVAS, Álex (2017). *Agente Encubierto Online*. Tesis de pregrado. Universitat Autònoma de Barcelona. p. 36.
[132] HERNÁNDEZ, M. (2019). *Inteligencia artificial y Derecho penal*. En Actualidad Jurídica Iberoamericana Nº 10 bis, junio. España, Instituto de Derecho Iberoamericano. p. 813.

ha estudiado la necesidad de introducir el mecanismo del agente encubierto cibernético en la legislación ecuatoriana. Refiere en este sentido que:

"*La intervención de* un *agente encubierto que ya no se encuentra limitado a una circunscripción territorial, sino que pasa a ser un agente encubierto cibernético, digital, online, o informático, ejecuta la operación encubierta en un espacio cibernético o virtual, caracterizado por ser ilimitado, exuberante y acéntrico. Sus actuaciones en este entorno de algoritmos y claves alfanuméricas, no colocan su vida en peligro o en riesgo físico por la latente posibilidad de ser identificado, sino que tendrá una identidad virtual, que se nutre el anonimato propicio de Internet*[133]".

Claro está que en este caso la autora analiza la figura del agente encubierto cibernético sin incluir la de los *bots* como especie de *software*, sino que se refiere a la actuación del agente encubierto como una persona real mediante el empleo de medios informáticos. Sin embargo, la autora da cuenta en este sentido de la necesidad de incluir una regulación de este tipo de agente en la legislación ecuatoriana en el marco de los métodos especiales de investigación penal, en vista de la importancia del empleo tecnológico en favor de la persecución criminal.

En el caso de Chile tenemos que el año 2017 se ratificó el Convenio Europeo sobre cibercriminalidad, conocido como Convenio de Budapest, en el cual se establece un marco general para la sanción e investigación de la cibercriminalidad, introduciéndose nuevos tipos penales, así como nuevas normas procesales que adecuan la investigación penal. La generalidad de este convenio no parece dar cuenta propiamente de la inclusión del mecanismo del agente encubierto cibernético o de los *bots* como medio de investigación o medio probatorio directamente.

Sin embargo, somos de la opinión que la adaptación del sistema normativo interno de Chile a dicho convenio sí puede contener normas relativas a este tipo de agente encubierto como forma especial de investigación, especialmente por el mandato contenido en el artículo 14, numeral l del convenio, que establece disposiciones comunes sobre el ámbito de aplicación de las medidas de Derecho procesal, señalando que "*Los Estados firmantes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y*

[133] PROAÑO, G. (2018). *La necesidad de incorporar al agente encubierto cibernético en la Legislación Ecuatoriana.* Iuris Dictio, Revista de Derecho. Volumen 22: 217-228.

procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos".

De tal manera que, al no enunciarse taxativamente cuáles habrán de ser los medios de investigación y los medios probatorios subsecuentes, la introducción a nuestro sistema de los agentes encubiertos cibernéticos y *bots* parece del todo posible, resultando idónea al espíritu del convenio ratificado, como un medio claro de modernizar la investigación penal del cibercrimen.

Tratándose del *common law* pareciera que el desarrollo legislativo relacionado con los medios informáticos se ha dirigido especialmente a la regulación de los documentos electrónicos en el ámbito probatorio, de manera similar a lo ocurrido con la Ley Nº 19.799 en Chile. Según Taruffo los países del *common law* hubieron asimilado los documentos electrónicos al testimonio de oídas, por no estar este medio probatorio al alcance directo del juez. Señala así que, respecto de Estados Unidos, los tribunales "*crearon una nueva excepción a la regla del testimonio de oídas al admitir pruebas informáticas, aunque su fuente original no pueda ser contrainterrogada. Así, la regla 803 (6) de las Federal Rules of Evidence se interpreta que incluye las pruebas electrónicas entre los archivos o grabaciones*[134]".

Asimismo, respecto del Reino Unido, Taruffo señala que se hubo admitido la procedencia de los documentos electrónicos, tratándolos como cualquier tipo de documento y presumiendo su autenticidad[135].

De tal manera, el autor concluye que "*en ambos sistemas se ha establecido la admisibilidad de las pruebas informáticas, abandonando reglas tradicionales de exclusión, y que la fiabilidad de tales pruebas se ha garantizado exigiendo que cumplan condiciones especiales en relación con el funcionamiento y el uso de los ordenadores*[136]".

Con todo, el ámbito de procedencia de la prueba informática al que alude Taruffo pareciera homologar el concepto amplio de prueba informática con el concepto específico de documento electrónico. Si bien lo anterior podría llevar a conclusiones terminológicamente incorrectas, de cierto podría señalarse que el documento electrónico es un caso de prueba informática por antonomasia. En efecto, en Inglaterra, pese a que las *Civil Evidence Act* de 1968

[134] TARUFFO, M. (2008). *op. cit*. p. 86.
[135] Ibídem. p. 86.
[136] Ibídem. p. 86.

y de 1995 regulan los documentos electrónicos, de cierto no regulan otros tipos de medio probatorios informáticos, como tampoco lo hace la *The Service of Documents and Taking of Evidence in Civil and Commercial Matters Regulations* del año 2018.

Finalmente, el instrumento jurídico internacional de mayor envergadura que se ha desarrollado para combatir el cibercrimen corresponde al Convenio sobre la Ciberdelincuencia o Convenio de Budapest. A pesar de que este instrumento establece nuevos tipos penales relacionados con la informática, así como medios procesales para su juzgamiento, de cierto deja abierto a cada Estado la adaptación de su Derecho interno para desarrollar medios de investigación apropiados para los delitos que sanciona.

Así, este convenio no aborda directamente el concepto de prueba informática, ni tampoco el de agente encubierto cibernético o *bots*, pero de cierto deja abierta la posibilidad de emplear estos medios como parte de los medios de investigación necesarios para perseguir y acreditar la comisión de ciertos delitos, lo que necesariamente deberá llevar un trabajo legislativo respecto de su empleo como medio probatorio en juicio.

6. Propuestas de cambio en la legislación chilena

Uno de los puntos más complejos de la problemática relativa a la procedencia de los *bots* como medio de prueba dice relación con la multiplicidad de los medios informáticos actualmente existentes.

En materia de documentos electrónicos, la Ley Nº 19.799 se ocupó de clarificar que estos tienen mérito probatorio, en los términos siguientes según su artículo 5º:

"*1.- Los señalados en el artículo anterior* (documentos electrónicos que tengan calidad de instrumento público)*, harán plena prueba de acuerdo con las reglas generales, y*

2. Los que posean la calidad de instrumento privado, en cuanto hayan sido suscritos con firma electrónica avanzada, tendrán el mismo valor probatorio señalado en el número anterior. Sin embargo, no harán fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador acreditado.

En el caso de documentos electrónicos que posean la calidad de instrumento privado y estén suscritos mediante firma electrónica, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales".

Asimismo, tenemos que el Código de Procedimiento Civil establece algunas consideraciones sobre la presentación de medios electrónicos en el proceso. Es el caso del artículo 348 bis. que regula la audiencia de percepción documental, estableciendo que:

"*Presentado un documento electrónico, el Tribunal citará para el 6° día a todas las partes a una audiencia de percepción documental. En caso de no contar con los medios técnicos electrónicos necesarios para su adecuada percepción, apercibirá a la parte que presentó el documento con tenerlo por no presentado de no concurrir a la audiencia con dichos medios*".

En este sentido, es claro el avance que el legislador ha desarrollado en la comprensión de estos medios probatorios, como queda de manifiesto en el inciso final de la norma citada, que excluye la procedencia de la audiencia de percepción documental cuando los documentos electrónicos puedan ser percibidos directamente en el expediente electrónico, en consideración del estado actual de la tramitación de los procesos en cuanto a la inclusión tecnológica.

Si bien es difícil pensar que nuestra legislación pueda regular cada uno de los medios electrónicos existentes de manera particular, en vista de su diversidad y particularidades propias, no es menos cierto que la situación es diferente en materia civil que en materia penal. Mientras en materia civil se enumeran los medios probatorios, entre los cuales debiéramos fijar la atención precisamente en la prueba instrumental, en materia penal se consagra un sistema de mayor libertad probatoria. En ese caso debiéramos preguntarnos si estamos en el ámbito de los instrumentos o debiéramos establecer una categoría intermedia, como el agente encubierto electrónico previsto en otras legislaciones.

Entonces, pese a que es deseable esperar una regulación especializada para regular el valor legal y procesal de cada uno de los avances tecnológicos existentes, tratándose de materias probatorias parece ser que un tratamiento genérico de los medios de prueba resulta más viable desde el punto de vista de la técnica legislativa. Creemos que son dos las posibilidades para lograr lo anterior. La primera, mediante la regulación expresa y genérica del valor probatorio de los medios informáticos, y otra mediante el establecimiento de principios probatorios generales que tiendan a la flexibilidad de su procedencia.

En cuanto a la regulación genérica de las tecnologías informáticas y su incidencia jurídica, una vía posible corresponde a la técnica legislativa que se hubo elegido en el caso de la Ley Nº 19.223, que tipifica figuras penales relativas a la informática. Su artículo 1º establece que "e*l que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo*".

En este caso se empleó la expresión "sistema de tratamiento de información". Pese a no definirse qué debe entenderse por tal, creemos que la redacción tiene la virtud de ser omnicomprensiva de diversas tecnologías informáticas, de manera que su ámbito de aplicación puede extenderse a la punibilidad de diversos hechos ilícitos. De la misma manera, resultaría un avance legislativo relevante que se regulara de una manera general similar la procedencia y valor de los medios probatorios informáticos.

En todo caso, parece necesario referir que dicha regulación legislativa podría darse mediante la dictación de una nueva ley que regule el cibercrimen en su conjunto o mediante la adaptación de la actual ley sobre delitos informáticos al Convenio contra el Cibercrimen.

En segundo lugar, tenemos que una posible solución puede encontrarse en el establecimiento de un sistema de libertad probatoria, como el del artículo 295 del Código Procesal Penal. Es también el caso de la Ley Nº 19.968, que crea los Tribunales de Familia, y que reza al tenor "*Todos los hechos que resulten pertinentes para la adecuada resolución del conflicto familiar sometido al conocimiento del juez podrán ser probados por cualquier medio producido en conformidad a la ley*".

Sin embargo, no resulta suficiente el establecimiento de un principio de libertad probatoria en normas procesales especiales como la citada, por cuanto su aplicación se encuentra restringida a las materias especiales correspondientes. De esta manera, como los procedimientos civiles se rigen por una restricción probatoria que no permite aplicar los medios informáticos como medios probatorios de manera general, sería necesario establecer un principio de libertad probatoria en cada ley procesal correspondiente.

Con todo, ello no obsta a que en lo presente concluyamos la procedencia general de los *bots* como medio probatorio, toda vez que su aplicación se concentrará más bien en los procesos penales, donde la libertad probatoria ya se encuentra consagrada.

Ante las interrogantes sobre la procedencia y eficacia de los *bots* como medio probatorio, tenemos que las respuestas son divergentes. Sobre la primera tenemos que la procedencia de los *bots* como probanza dependerá del procedimiento que se trate. Tratándose del procedimiento civil, este medio no permitirá, teóricamente, probar las alegaciones de las partes, en virtud de la restricción probatoria del artículo 341 del Código del ramo, por cuanto sería más bien artificioso elaborar alguna asimilación a los medios establecidos.

En el caso del proceso penal, del proceso laboral y del proceso de familia, en que el acoso puede configurarse como sustrato fáctico del proceso, tenemos que las partes sí podrán valerse de los medios informáticos en general, y de los *bots* en particular, como medio de prueba, en vista de la libertad probatoria existente y de la posibilidad de asimilación de los medios de prueba atípicos a aquellos regulados por la ley.

Finalmente, al margen del camino legislativo que se emplee para propiciar el uso de la prueba informática en el ámbito procesal, lo que resulta claro es la necesidad de adoptar medidas que tiendan a la cooperación de la tecnología y la informática al mejor desarrollo de la jurisdicción.

CONCLUSIONES

Las redes sociales y las aplicaciones de mensajería instantánea, cuyo uso se ve aumentado con el pasar de los años -todo ello gracias al desarrollo de la tecnología y la consecuente masificación de Internet- han llevado a otro nivel las relaciones humanas, siendo estas cada vez más rápidas y sencillas, facilitando de este modo la vida de sus usuarios, quienes emplean estas herramientas de manera diaria y constante, tanto en el ámbito social, como laboral o académico.

Estos distintos usos que se le asigna por parte de los usuarios a las redes sociales es un punto que merece especial atención, toda vez que, si bien estas han sido creadas con fines tales como facilitar la comunicación entre particulares, ayudar a la difusión de información de interés público, promocionar negocios o servicios, etc., también se han visto envueltas en polémicas debido al uso malicioso dado por sus propios usuarios, surgiendo así una evolución del conocido fenómeno del "acoso" o "*bullying*", llegando este a efectuarse mediante los nuevos canales de comunicación para dar lugar al llamado "ciberacoso" o "*ciberbullyin*g".

De manera diaria, cientos de usuarios, muchos de ellos niños en edad escolar, reciben mensajes de sus pares o de desconocidos a través de la red, los cuales llevan consigo una intención de causar temor o humillación en la persona víctima de esta acción.

Producto de la masificación de este fenómeno y sus negativos efectos en la población, los cuales incluyen bajo rendimiento escolar, ansiedad, depresión, pensamientos suicidas, etc., este ha estado en el punto de mira de diversas entidades, con la finalidad de regular estas conductas. Entre ellos podemos destacar el esfuerzo del Ministerio de Educación, que impulsó la creación de la Ley de Violencia Escolar (Ley N° 20.536), pero que tan solo implica una regulación cuya aplicación no es más que a través de reglamentos internos en centros educacionales. Del mismo modo, más allá del ámbito escolar, se destacan proyectos que han tratado de sancionar penalmente actos que, si bien no aluden abiertamente al ciberacoso, constituyen un subtipo de acoso a través de la red, tal como la difusión de fotos íntimas a través de Internet sin el consentimiento de su propietaria, la cual trata de sancionarse mediante un Proyecto de Ley impulsado por el Ministerio de la Mujer y Equidad de Género, con multas de hasta 20 Unidades Tributarias Mensuales.

En vista de lo señalado, se hace necesario hallar métodos eficaces para combatir esta nueva forma de acoso. Dentro de ellas, una opción que podría ser factible será el empleo de *bots* o de agentes encubiertos electrónicos para la detección del ciberacoso.

Los *bots* pueden definirse como *softwares* creados con la intención de simular el comportamiento humano, con el objeto de realizar diversas tareas de manera repetitiva.

Desgraciadamente, hasta la actualidad, Chile no cuenta con una regulación expresa que estipule el alcance y profundidad de la labor de los *bots*. Adicionalmente, al no tratarse de personas humanas las que llevarían a cabo esta labor de detectar y prevenir el ciberacoso, estos *bots* encuentran diversos obstáculos, puesto que existen limitaciones lingüísticas para la detección de ciertas palabras, debido a que estos debieran ser configurados en la mayor variedad de idiomas posible, siendo que en la actualidad el repertorio es más bien reducido.

Pero más importante aún para el caso de Chile en particular es la posibilidad de que estos *softwares*, que serían programados para la detección de determinadas palabras o frases, deben tener en consideración la ortografía de las palabras dentro de un mismo idioma, puesto que las redes sociales, tratándose estas de medios de comunicación más bien informales, sus usuarios no necesariamente respetarán las reglas ortográficas del idioma, pudiendo recurrir a una escritura alterna de la palabra con el propósito de evitar la censura, o incluso a imágenes en las cuales se contengan textos que puedan ser ofensas directas al receptor de estas.

Debido a estas dificultades, se requiere un *bot* programado con altas capacidades de comprensión del lenguaje natural para hacer frente a estos obstáculos, aunque todo ello puede lograrse mediante grandes esfuerzos informáticos y programadores altamente capacitados para cumplir con esta tarea.

Por su parte, el agente encubierto consiste en la intromisión de un funcionario policial encubierto en un grupo organizado, con el fin de detectar la comisión de delitos, reunir pruebas de este y lograr una sanción para sus autores. La prueba obtenida por dicho agente será utilizada en el proceso penal.

En la actualidad, el empleo de esta figura es aceptada en múltiples ordenamientos jurídicos, dentro de los cuales se incluye Chile, pero que, como punto en contra, tan solo está

regulada respecto de delitos en contra de organizaciones criminales, tráfico de drogas o aquellos delitos contra menores de edad relacionados con pornografía y prostitución, no estando contemplado para situaciones de ciberacoso, pero que, de ser así, podría constituir una eficaz herramienta para erradicarlo, toda vez que es una figura ya aceptada e incorporada en nuestro ordenamiento jurídico.

Estos medios señalados podrían, entonces, emplearse como un potente medio probatorio para evitar, detectar y sancionar el ciberacoso.

Para entender los *bots* como medios probatorios es necesario analizar la procedencia de las tecnologías que no están previstas expresamente en la ley como medio de prueba. Tratándose del proceso civil cabe concluir que los *bots* no se encuentran expresamente aceptados. La falta de una referencia general a la inclusión de medios probatorios electrónicos incide en que debamos descartar su procedencia directa. Sin embargo, al diferenciar entre la fuente probatoria y la probanza misma, es posible obtener como corolario que su procedencia y uso puede subsumirse en el desarrollo de la prueba documental, bajo la especie de los documentos electrónicos, según lo estipula la ley Nº 19.799; así como al desarrollo de la prueba pericial. Luego, la falta de una regulación directa no es óbice para admitir su procedencia.

En relación a la procedencia de los instrumentos informáticos como medio probatorio, en el caso de los *bots* en relación al proceso penal, esta debe ser completamente aceptada, toda vez que el Código Procesal Penal establece el principio de libertad probatoria y, a su vez, la ley establece que el tribunal podrá asimilar un medio de prueba no contemplado en la ley a otro análogo que cuente con recepción legal, con el único requisito de cumplir con una carga procesal, correspondiente a proporcionar los medios tecnológicos necesarios para la incorporación de dicho medio de prueba.

Como medio probatorio, los *bots* requerirían de un informe pericial, por la razón de que la presentación de los *bots* corresponde a un instrumento informático, requiriéndose por ello de un experto en dicha materia para incorporar este medio al proceso y, posteriormente, se deberá acreditar los hechos constitutivos de ciberacoso y la información recabada por estos *bots*.

Al contrario de lo que ocurre con los *bots*, la prueba respecto al agente encubierto no tiene mayor complejidad, toda vez que esta figura ya se encuentra incorporada y regulada en Chile. Por tanto, en el eventual caso de ser posible ampliar la lista de delitos susceptibles de ser

investigados por un agente encubierto, añadiendo el ciberacoso, en la mayoría de los casos esta prueba sería aceptada por el juez si este hubiera autorizado previamente la utilización de este medio de investigación, lo cual es un requisito esencial, toda vez que la investigación realizada por un agente encubierto implica una vulneración de derechos de la parte investigada. De lo contrario, en caso de no haber existido autorización judicial previa, o en el supuesto de que el agente encubierto se haya excedido en sus funciones, la defensa podría objetar la prueba y que esta se declarase como prueba ilícita. Dicho de otro modo: la autorización del juez en el empleo de este medio legitima la transgresión de ciertos derechos fundamentales en pos de recabar pruebas para el proceso penal.

De este modo, en lo relacionado al agente encubierto electrónico, el ordenamiento jurídico chileno no requiere grandes modificaciones, sino que tan solo deja ver una necesidad de hacer extensiva esta figura a otro tipo de delitos de difícil investigación por otros medios, como el ciberacoso, debido a que este atenta contra bienes jurídicos importantes de proteger, siempre respetándose el principio de subsidiariedad, el cual implica el empleo de esta técnica solo en caso de no existir otros medios de investigación o si estos no fueron exitosos.

Sin embargo, si quisiéramos incorporar los *bots* como medio de prueba, sí podemos observar la necesidad de proponer diversos cambios en la legislación chilena.

A pesar de que sería ideal que el legislador pudiese regular el valor legal y procesal de cada instrumento informático que surja debido a los avances tecnológicos, resulta evidente que esto no es posible, siendo más viable un tratamiento genérico de estos medios de prueba. Para ello, observamos dos vías mediante las cuales podría lograrse: primeramente, mediante la regulación expresa y genérica del valor probatorio de los medios informáticos; y otra mediante el establecimiento de principios probatorios generales que tiendan a la flexibilidad de su procedencia.

Respecto a la regulación expresa y genérica de las tecnologías informáticas y su incidencia jurídica, en caso de optar por esta vía, se requeriría tipificar aquellas figuras penales relativas a la informática. Esta regulación podría conseguirse a través de la dictación de una nueva ley que regule el cibercrimen, o mediante la adaptación de la actual ley sobre delitos informáticos del Convenio contra el Cibercrimen.

En referencia a la segunda vía señalada, es decir, el establecimiento de principios probatorios generales que tiendan a la flexibilidad de su procedencia, esto podría lograrse mediante la implementación de un sistema de libertad probatoria, aceptándose de esta forma cualquier medio de prueba en conformidad a la ley que permita probar los hechos.

A pesar de lo señalado, y en consideración a que la implementación de *bots* como medio de prueba que señalamos sería principalmente aplicable al proceso penal, en el cual ya existe la libertad probatoria, este medio de prueba debiera ser completamente aceptado, pudiendo las partes valerse de los medios informáticos -incluyendo el empleo de *bots*- como medio de prueba, en vista de la libertad probatoria existente y de la posibilidad de asimilación de los medios de prueba atípicos a aquellos regulados por la ley.

En conclusión, más allá de la vía legislativa elegida para lograr respaldo del empleo de la prueba informática en materia procesal, se puede evidenciar la clara necesidad de adoptar las medidas que sean requeridas para que las nuevas tecnologías puedan lograr grandes mejoras al sistema judicial.

BIBLIOGRAFÍA

I. LIBROS

1. CAFFERATA, J. (2003). *La prueba en el proceso penal* (5º edición). Buenos Aires, Editorial Depalma.
2. CARBONELL, F. (2018). *Sana crítica y razonamiento judicial*. En BENFELD, J. y LARROUCAU, J. (eds.), *La sana crítica bajo sospecha*. Valparaíso, Ediciones Universitarias de Valparaíso.
3. CASARINO, Mario (1911). *Manual de Derecho Procesal. Derecho Procesal Civil*. Tomo IV. Santiago, Editorial Jurídica de Chile, 2009.
4. CAVADA H. Juan Pablo, "*Revenge Porn. Legislación extranjera*". Biblioteca del Congreso Nacional de Chile. Asesoría Técnica Parlamentaria. Diciembre, 2018, Nº SUP 118573. En línea en https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26729/1/Revenge_porn_en_la_legislacion_extranjera.pdf [consulta: 10.05.2021]
5. CHAHUÁN, S. (2002). *Manual del nuevo procedimiento penal*. 2° edición. Santiago, Lexis Nexis.
6. COUTURE, E. (1958). *Fundamentos del Derecho Procesal Civil*. 4° edición. Buenos Aires, Editorial Metropolitana.
7. DÍAZ, M. (2017). *Manual de procedimiento del trabajo.* Santiago, Librotecnia.
8. DÍAZ, S. (2018). *Robots y responsabilidad civil*. Madrid, Reus Editorial.
9. ERCILLA, J. (2018). *Normas de Derecho Civil y Robótica: Robots inteligentes, personalidad jurídica, responsabilidad civil y regulación*. Pamplona, Thomson Reuters Arazandi. 224 pp.
10. HORVITZ, M. y LÓPEZ, J. (2004). *Derecho Procesal Penal Chileno*. Tomo II. Santiago, Editorial Jurídica de Chile.

11. MONTOYA, M. (2001). *Informantes y técnicas de investigación encubiertas*. Análisis Constitucional y Procesal Penal. 2ª edición. Buenos Aires, Paidós.

12. MUÑOZ, J. (1995). *La moderna problemática jurídico penal del agente provocador*. Valencia, Tirant lo Blanch.

13. RIQUELME, E. *op. cit*., p. 8; MONTOYA, M. *op. cit*., p. 79, 153; RENDO, Á. o*p. cit.*; y ARCINIEGAS, G. *op. cit*.

14. SOTO, F. (1989). *El delito de tráfico ilegal de drogas*. Madrid, Editorial Trivium S.A.

15. TARUFFO, M. (2008). *La prueba*. Madrid, Marcial Pons.

16. VALLE, F.et al (2020). *Delitos de acoso genérico, acoso y chantaje sexual*. Breña, Pacífico Editores S.A.C.

II. ARTÍCULOS Y PUBLICACIONES SERIADAS

1. AGUIRREZÁBAL, M. (2011). *La imparcialidad del dictamen pericial como elemento del debido proceso*. *Revista chilena de derecho*, 38(2).

2. BARBOZA G. (2018). *The association between school exclusion, delinquency and subtypes of cyber- and F2F-victimizations: identifying and predicting risk profiles and subtypes using latent class analysis*. *Child Abuse Negl*. Citado por TORRES-MONTILLA, Y., en "Características del ciberacoso y psicopatología de la víctima". Repertorio de Medicina y Cirugía 27(3).

3. BORJA, E. (2003). *Sobre el concepto de política criminal*. *Una aproximación a su significado desde la obra de Claus Roxin*. Anuario de derecho penal y ciencias penales (España). 56(1).

4. CASTRO, C. et al(2019). Revista de Psicología y Ciencias del Comportamiento de la Unidad Académica de Ciencias Jurídicas y Sociales.. 10(2).

5. DEL POZO, M. (2006). *El agente encubierto como medio de investigación de la delincuencia organizada en la Ley de Enjuiciamiento Criminal Española*. Criterio jurídico, 6.

6. GUTIÉRREZ, Ainhoa (2019). *Ciberacoso sexualizado y ciberviolencia de género en adolescentes*. Nuevo marco regulador para un abordaje integral. R.E.D.S. 14.

7. HERNÁNDEZ, María (2019). *Inteligencia artificial y Derecho penal*. En Actualidad Jurídica Iberoamericana Nº 10 bis, junio. España, Instituto de Derecho Iberoamericano.

8. HÜTT, H. (2012). *Las redes sociales: una nueva herramienta de difusión.* Reflexiones (Universidad de San José de Costa Rica),91(2).

9. JOFFRE, V. M. et al (2011). *Bullying en alumnos de secundaria, características generales y factores asociados de riesgo.* Boletín Médico del Hospital Infantil de México 68(3).

10. PEDICONE, F. (2001). *¿Derecho Penal clásico vs. Derecho Penal moderno?*. Revista de la Policía Federal Argentina. Octubre.

11. PEÑA, A. (2011). *El nuevo proceso penal peruano*. Lima, Gaceta Jurídica.

12. PROAÑO, G. (2018). *La necesidad de incorporar al agente encubierto cibernético en la Legislación Ecuatoriana.* Iuris Dictio, Revista de Derecho. 22.

13. REDONDO, J., et al (2017). *Impacto psicológico del ciberbullying en estudiantes universitarios: un estudio exploratorio*. Revista Colombiana de Ciencias Sociales, 8 (2).

14. SANTOS, M. (2007). *Regulación legal de la robótica y la inteligencia artificial: retos de futuro*. Revista Jurídica de la Universidad de León.4.

15. SMOKOWSKI, P. R. y KOPASZ, K. H. (2005). *Bullying in school: An overview of types, effects, family characteristics, and intervention strategies. Children and Schools*. 27 (2).

16. TIRADO, Carmen (2020). *¿Qué es un robot? Análisis jurídico comparado de las propuestas japonesas y europeas*. En Mirai, Estudios japoneses (Universidad Complutense de Madrid). 4.

17. VEGA-OSES, A.y PEÑALVA-VÉLEZ, A. (2018). *Los protocolos de actuación ante el acoso escolar y el ciberacoso en España: un estudio por comunidades autónomas*. International Journal of New Education (Universidad de Málaga). Número 1.

III. JURISPRUDENCIA

Corte Suprema. Tercera Sala (Constitucional). Rol Nº 3075-2005. Santiago, Chile.

IV. LEGISLACIÓN

1. Código de Procedimiento Penal, artículo 242. Colombia.
2. Código Federal, art. 885-d. Estados Unidos.
3. Código Orgánico Integral Penal. Ecuador.
4. Código Penal. Chile.
5. Código procesal penal de Colombia. Recurso electrónico disponible en el sitio online de la Defensoría Penal de Colombia, https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_906_2004.pdf.
6. Código Procesal Penal de la Nación. Ministerio de Justicia y Derechos Humanos. Buenos Aires, Sistema Informático Argentino de Información Jurídica, 2014.
7. Convención sobre los Derechos del Niño. 1989.
8. Convenio sobre la Ciberdelincuencia: Convenio de Budapest. Biblioteca del Congreso Nacional de Chile, BCN. Julio 2018.
9. Ley N 19.293 Código del Proceso Penal (Uruguay. Disponible en el sitio online de la Fiscalía General de la Nación, http://www.fiscalia.gub.uy/innovaportal/v/1092/1/innova.front/leyes.html.

10. Ley N° 19.574, ley integral contra el lavado de activos (Uruguay). Disponible en sitio online de IMPO, Centro de Información Oficial, Sección de Normativa y Avisos Legales del Uruguay, impo.com.uy.
11. Ley de Enjuiciamiento Criminal. España. Recurso electrónico disponible en el sitio online de la Agencia Estatal Boletín Oficial del Estado (España) https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036.
12. Ley Nº 20.000, Ley de Drogas. Chile.
13. Ley Nº 20.370, General de Educación. Chile.
14. Ley Nº 20.526, Sanciona el acoso sexual de menores, la pornografía infantil, virtual y la posesión de material pornográfico infantil. Chile.
15. Ley Nº 20.536, Ley de Violencia Escolar. Chile.
16. Ley Nº 27.319 sobre Investigación, Prevención y Lucha de los delitos complejos. (Argentina). Recurso electrónico disponible en el sitio online del gobierno argentino, http://servicios.infoleg.gob.ar/infolegInternet/anexos/265000-269999/268004/norma.htm
17. Ley Nº 29.719. Perú.

V. DOCUMENTOS DE ORGANISMOS INTERNACIONALES

1. Comité de derechos del Niño. Observaciones Generales del Comité de Derechos del Niño. Observación General Nº 14.
2. Normas de Derecho Civil sobre robótica. *Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)).* P8_TA (2017) 0051. [En línea] en https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.pdf?redirect [consulta: 18.07.2020].
3. OAS. *Relatoría sobre los Derechos de las personas Lesbianas, Gays, Bisexuales, Trans e Intersex y la Relatoría Especial para la Libertad de Expresión de la CIDH*. Capítulo

IV. Discurso de Odio y la Incitación a la violencia contra las personas lesbianas, gays, bisexuales, trans e intersex en América. [en línea] Aprobado por la Comisión Interamericana de Derechos Humanos el 12 de noviembre de 2015. http://www.oas.org/es/cidh/expresion/docs/informes/odio/Discurso_de_odio_incitacion_violencia_LGTBI.pdf [consulta: 06.04.2021].

4. Recomendación nº 15 de la Comisión Europea contra el Racismo y la Intolerancia (ECRI) del Consejo de Europa. 2015.

VI. NOTICIAS

1. Cooperativa.cl. *Mineduc creará bot para combatir ciberacoso entre escolares.* Noviembre 2018. [En línea] en https://www.cooperativa.cl/noticias/pais/educacion/violencia-escolar/mineduc-creara-bot-para-combatir-ciberacoso-entre-escolares/2018-11-04/110956.html [consulta: 06.04.2021].

2. La Tercera. *Mineduc crea bot para enfrentar el ciberacoso en redes sociales*. Noviembre 2018. [En línea] en https://www.latercera.com/nacional/noticia/mineduc-crea-bot-para-enfrentar-el-ciberacoso-en-redes-sociales/386876/ [consulta: 17.04.2021].

3. New Robot Strategy. *Japan's Robot Strategy*. [En línea] en http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf. [04.05.2021].

VII. RECURSOS ELECTRÓNICOS

1. ABC Educación. *Muchas víctimas de ciberbullying no acuden a sus familiares a por ayuda*. 2016. [En línea] en https://www.abc.es/familia/educacion/abci-muchas-victimas-ciberbullying-no-acuden-familiares-ayuda-201612071105_noticia.html [consulta: 10.07.2020].

2. ARRIAGADA, J. Y CALZON, B. *Ciberacoso: Violencia de género a un solo clic*. *Reportaje sobre el acoso y las humillaciones a mujeres en redes y plataformas digitales*.

Mayo 2019. [En línea] en https://vergara240.udp.cl/ciberacoso-violencia-de-genero-a-un-solo-clic/ [consulta: 17.04.2021].

3. Blog de Inbenta. *Chatbots: ¿buenos o malos imitadores de la interacción humana?* 08 de mayo de 2019. [En línea] en https://www.inbenta.com/es/blog/chatbots-buenos-o-malos-imitadores-de-la-interaccion-humana/ [consulta: 25.09.2020].
4. Centro de Estudios MINEDUC. *Acoso: una revisión internacional y nacional de estudios y programas*. Santiago, Chile. 2018. [En línea] https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf. [consulta: 25.03.2021].
5. Conecta software. [En línea] en https://conectasoftware.com/glosario/bot-botnet/ [consulta: 15.07.2020]
6. DÍAZ, J. (2012) "*Una aproximación al concepto de discurso del odio*" en Rev. Derecho Estado [online]. 2015, nº 34. ISSN 0122-9893. http://dx.doi.org/10.18601/01229893.n34.05, citando a Jeremy Waldron. The harm in hate speech, London, Harvard University Press, 2012 p.105-146 [consulta: 15.09.2020].
7. Digital Guide IONOS. *Direcciones IP: Todo lo que debes saber.* 02 de Septiembre de 2020. [En línea] en https://www.ionos.es/digitalguide/servidores/know-how/direccion-ip/ [consulta: 01.10.2020].
8. FUMEY, Juan. *¿Existe una ley que nos proteja del ciberacoso?* Agosto 2018. [En línea] en https://www.bufetes.cl/articulos/existe-una-ley-que-nos-proteja-del-ciberacoso [consulta: 12.07.2020].
9. GUEVARA, Javier; STHIOUL, Alberto; RIVERA, Mario; BARRIENTOS, Fernando. *Ciberacoso: una revisión internacional y nacional de estudios y programas*. Centro de Estudios Mineduc. Evidencias Nº 43. Noviembre 2018. [En línea] en https://centroestudios.mineduc.cl/wp-content/uploads/sites/100/2018/11/EVIDENCIAS-43.pdf [consulta: 06.07.2020].
10. GUTIÉRREZ, Camilo. *Inteligencia artificial para detectar cyberbullying en Twitter*. Agosto 2012. [En línea] en https://www.welivesecurity.com/la-

es/2012/08/14/inteligencia-artificial-detectar-cyberbullying-twitter/ [consulta: 06.04.2021].

11. INTECO. *Estudio sobre hábitos seguros en el uso de las TIC por los menores*. 2009. [En línea] https://faros.hsjdbcn.org/es/noticia/estudio-sobre-habitos-seguros-uso-tic-ninos-adolescentes-confianza-padres. [consulta: 06.04.2021].
12. KENNEDY SHRIVER, Eunice. *National Institute of Child Health and Human Development*. *Focus on children's mental health research at the NICHD.* 2012. [En línea] en https://www.nichd.nih.gov/newsroom/resources/spotlight/060112-childrens-mental-health [consulta: 09.07.2020].
13. Legislatura del Estado de Washington. [En línea]. Disponible en, https://app.leg.wa.gov/RCW/dispo.aspx?cite=28A.300.285. [consulta: 24.05.2021].
14. MINISTERIO DE EDUCACIÓN, Argentina. Presidencia de la Nación. *Robótica: Entrá al mundo de la inteligencia artificial*. Conectados, La revista. Argentina. [En línea] https://issuu.com/eslibre.com/docs/rob__tica__entra_al_mundo_de_la_int. [consulta: 09.04.2021].
15. NAVARRETE, María José. *Mineduc crea bot para enfrentar el ciberacoso en redes sociales.* La Tercera. 04 de noviembre de 2018. [en línea] https://www.latercera.com/nacional/noticia/mineduc-crea-bot-para-enfrentar-el-ciberacoso-en-redes-sociales/386876/ [consulta: 17.07.2020].
16. ONU. "*La estrategia y plan de acción de las naciones unidas para la lucha contra el discurso de odio".* [En línea] en https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_ES.pdf [consulta: 06.04.2021].
17. SEMAL. *La importancia de prevenir el bullying y ciberbullying*. Marzo 2017. [En línea] en https://www.semal.org/es/component/k2/la-importancia-de-prevenir-el-bullying-y-ciberbullying [consulta: 06.04.2021].
18. Senado de Nueva York. [En línea]. Disponible en https://www.nysenate.gov/legislation/laws/CONSOLIDATED. [consulta: 24.05.2021].

19. STOPBULLYING (Gobierno de Estados Unidos). [En línea] Disponible en https://www.stopbullying.gov/resources/laws/federal. [consulta: 24.05.2021]

20. TORRES-MONTILLA, Yormar, en "*Características del ciberacoso y psicopatología de la víctima*", En Repertorio de Medicina y Cirugía. Vol. Nº 27, Nº 3, 2018 [En línea] en https://www.fucsalud.edu.co/sites/default/files/2018-11/Art-10.pdf [consulta: 09.04.2021].

21. TORRES MUÑOZ, Rafael. *Políticas Públicas para la Robótica y la Inteligencia Artificial*. Biblioteca del Congreso Nacional de Chile / BCN. 2019. [En línea] https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/26982/1/Politicas_Publicas_para_la_Robotica_y_la_Inteligencia_Artificial.pdf. [consulta: 09.04.2021].

22. UNESCO. *Combatiendo el Discurso de Odio en Línea*. ISBN 978-92-3-1000105-5. 2015. [En línea] en https://unesdoc.unesco.org/ark:/48223/pf0000233231 [consulta: 06.04.2021].

23. WEIDENSLAUFER, Christine; MEZA-LOPEHANDÍA, Matías. *El ciberacoso escolar en el derecho penal: Formas de regulación en el derecho extranjero*. 2018. [En línea] en https://www.bcn.cl/obtienearchivo?id=repositorio/10221/25508/1/BCN2018___FINAL___Ciberacoso_en_la_legislacion_extranjera.pdf [consulta: 13.07.2020].

24. ZAVIDICH, Carolina. *El Agente Encubierto y su responsabilidad*. Unidad Especializada de Tráfico Ilícito de Estupefacientes y Sustancias Sicotrópicas. [En línea] en http://www.fiscaliadechile.cl/observatoriodrogaschile/documentos/publicaciones/articulo_25_ley_20000_agente_encubierto_CZ.pdf [consulta: 06.04.2021].

VIII. TESIS DE PREGRADO Y POSGRADO

1. CÁNOVAS, Álex (2017). *Agente Encubierto Online*. Tesis de pregrado. Universitat Autònoma de Barcelona.

2. CLUSA, Alejandro (2019). *El Agente encubierto informático*. Tesis de fin de grado. Universidad de Zaragoza.

3. PALOP. Melania (2017). *Protección jurídica de menores víctimas de violencia de género a través de internet*. Tesis Doctoral, dirigida por José Bonet Navarro, profesor de Derecho procesal. Universitat Jaume.

4. RUIZ ANTÓN, Luis Felipe (2015). *El agente provocador*. Tesis doctoral, Universidad Complutense de Madrid, Facultad de Derecho. Madrid, España.