Módulo 7

CIBERCRÍMENES

Serie de módulos sobre la defensa de la libertad de expresión

MEDIA DEFENCE

Publicado por Media Defence: www.mediadefence.org

Este módulo ha sido preparado con la ayuda de Fundación para la Libertad de Prensa: https://www.flip.org.co/index.php/es/

Tabla de contenidos

MÓDULO 7
CIBERCRÍMENES

- Aunque existen distintas normativas que castigan determinadas conductas como tal, no existe una definición legal y común sobre el cibercrimen a nivel interamericano. Empero, se acude a esta figura cuando las conductas afectan la integridad, confidencialidad y disponibilidad de la información contenida en sistemas informáticos, de redes o de datos y, además, cuando se hace uso indebido del Internet.

- En 2019, la exposición a riesgos cibernéticos era tan inevitable que América Latina y el Caribe se consolidó como un "objetivo y fuente de ataques cibernéticos"[1]. Como un ejemplo, en ese año, las economías de Brasil, Argentina y México fueron las más atacadas digitalmente a nivel global, ocupando Brasil el tercer lugar[2]. De forma paralela, en tan solo 2017, se registraron 177.500 ataques de malware por hora en América Latina[3].

- Por ello, la Organización de los Estados Americanos (OEA) ha considerado fundamental que los marcos jurídicos de los Estados interamericanos contengan leyes sustantivas sobre delitos cibernéticos y leyes procesales para la recopilación de la evidencia electrónica. Además de prever la cooperación técnica interestatal y con Grupos de Expertos sobre estos asuntos[4].

- Cada vez es más frecuente la intervención del Estado a partir de legislaciones que respondan a los cibercrímenes en asuntos que repercuten, incluso, de forma diferenciada en las mujeres y niñas que pueden ser víctimas de delitos cometidos en el espacio digital.

- Existe una tendencia en la región de criminalizar los discursos en línea, sobre todo ante contextos de contención social, a partir de la aplicación de leyes para combatir el crimen cometido en el escenario digital. Tal es el caso de la publicación y difusión de información falsa.

Introducción

Ante el avance creciente de las nuevas tecnologías a nivel global, los Estados de las Américas han tenido que resignificar sus prácticas hacia brindar una respuesta efectiva que responda a delitos

[1] OEA. Consideraciones de Ciberseguridad del proceso democrático para América Latina y el Caribe. 2019, pág. 21. En: https://www.oas.org/es/sms/cicte/docs/ESP-Cybersecurity-Democratic-Process-LAC.pdf
[2] Symantec, "2019 Internet Security Threat Report". Febrero 2019.
[3] Kapersky Lab. "33 ataques por Segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina". 2017. Disponible en: https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increasein-malware-attacks-in-latin-america
[4] OEA. Tercera Reunión del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, OEA/Ser.K/XXXIV, CIBER-III/doc.4/03).8 y OEA. Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética. Anexo A.

cibernéticos como la pornografía infantil, robo de datos, acoso cibernético, entre otros[5]. Según el Registro de Direcciones de Internet de América Latina y Caribe (LACNIC), las tendencias sobre ataques en ciberseguridad de la región permiten concluir que el cibercrimen se apropia del 15% al 20% de las economías que genera Internet en un año, siendo el phishing la principal amenaza cibernética registrada en la región[6].

De esta manera, le corresponde a los Estados garantizar un ciberespacio seguro que combata el cibercrimen como un asunto de máxima prioridad dentro de su política[7] y para ello, debe observar las reglas del derecho internacional, así como adoptar medidas de cooperación para "fortalecer sus sistemas de prevención, detección, alerta y respuesta a las amenazas en el ciberespacio"[8]. No obstante, dadas las circunstancias particulares de estas tecnologías, las estrategias de seguridad cibernética deben estar en armonía con los derechos fundamentales, tales como la privacidad, la libertad de expresión, el debido proceso, así como los principios de apertura, universalidad e interoperabilidad del Internet[9].

La complejidad que enfrentan las autoridades hoy en día para perseguir este tipo de delitos cibernéticos es cada vez más frecuente y se encuentra en constante evolución. La OEA adoptó por primera vez en 2003, una "Declaración sobre Seguridad de las Américas". En esta, se abordó la concepción de la seguridad desde un enfoque multidimensional, puesto que los ataques a la seguridad cibernética pueden ser de naturaleza transnacional y requieren de la cooperación de todos los Estados miembros[10].

Este fue el primer instrumento interamericano que reafirmó la necesidad de desarrollar una cultura de seguridad cibernética en las Américas que incluía adoptar medidas de prevención de ataques, luchar contra las amenazas cibernéticas y combatirlas a través de la tipificación de las mismas en la jurisdicción. Sin embargo, no se agotó allí. En 2004, la OEA creó la "Estrategia Interamericana de Seguridad Cibernética", por medio de la cual se amplió la protección de seguridad sobre redes y sistemas de información ante las amenazas que resultan de ataques maliciosos o delictivos[11].

Para desarrollar lo anterior, se previó que los Estados miembros de la OEA trabajarían de forma

[5] OEA. Comunicado C-063/16. Ciberdelito: 90.000 millones de razones para perseguirlo. Disponible en: https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-063/16#:~:text=Seg%C3%BAn%20estimaciones%20de-,LACNIC,-%2C%20el%20organismo%20que

[6] LACNIC. Tendencias sobre ataques en ciberseguridad en América Latina y el Caribe. 6 de noviembre de 2018. https://prensa.lacnic.net/news/ciberseguridad/tendencias-sobre-ataques-en-ciberseguridad-en-america-latina-y-el-caribe

[7] Naciones Unidas. Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. A/74/120. 24 de junio de 2019.

[8] Ibídem.

[9] Observatorio de la Ciberseguridad en América Latina y el Caribe. Ciberseguridad ¿estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016, pág. 7. Disponible en: https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

[10] OEA. Declaración sobre seguridad de las Américas. OEA/Ser.K/XXXVIIICES/dec.1/03 rev. 1. 28 de octubre de 2003. México.

[11] OEA. Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética. Resolución AG/RES.2004 (XXXIV-O/04). 8 de junio de 2004.

conjunta con las iniciativas del Comité Interamericano contra el Terrorismo (CICTE), la Comisión Interamericana de Telecomunicaciones (CITEL) y con el Grupo de Expertos Gubernamentales en materia de Delito Cibernético de las Reuniones de Ministros de Justicia o Ministros o Procuradores Generales de las Américas (REMJA) con el fin de disuadir "el uso indebido del Internet y los sistemas de información asociados e [impulsar] el desarrollo de redes de información que sean de confianza y fiables"[12].

Adicionalmente, la Organización de los Estados Americanos incluyó la necesidad de promulgar una legislación sobre delitos cibernéticos en el interior de los Estados bajo la asistencia de una mesa técnica y talleres regionales precedidos por el Grupo de Expertos en los que se concentraron en dos categorías de leyes:

1. Leyes sustantivas sobre delitos cibernéticos: por primera vez se habló de la fijación de tipos penales por los Estados sobre comportamientos que atenten contra la confidencialidad, la integridad y seguridad de los sistemas informáticos, tales como "el acceso a los computadores sin autorización, la interceptación ilícita de datos, la interferencia con la disponibilidad de sistemas informáticos y el robo y sabotaje de datos"[13].

2. Leyes procesales para la recopilación de pruebas electrónicas: de conformidad con lo anterior, los Estados deben consolidar un andamiaje institucional con estricto apego a normas internacionales para desempeñar labores de investigación de un delito que les permitan acceder y recabar comunicaciones y datos.

Así, el panorama regional parecía avanzar hacia el fomento mutuo de una confianza digital. No obstante, los ataques cibernéticos cada vez eran más frecuentes en la región. Estas tendencias corresponden entonces al crecimiento exponencial de las tecnologías en la región, lo cual, a su vez, insta a tener en cuenta dimensiones transversales que deben analizarse en la comisión de estos delitos, como el componente de género. La OEA ha documentado que los Estados han actualizado sus marcos jurídicos hacia la tipificación del ciberhostigamiento, el ciberacoso, el grooming y el ciberbullyng por ejemplo, así como la distribución no consentida de imágenes íntimas o sexuales[14].

Finalmente, desde Naciones Unidas se ha expresado la preocupación de que estas leyes y prácticas dirigidas a contrarrestar el crimen en el escenario digital, a menudo, vulneran libertades individuales de grupos de especial protección, de tal suerte que los Estados han acudido a limitar el derecho a la libertad de expresión en línea. Al respecto, la Relatoría Especial sobre el derecho a la libertad de reunión pacífica y asociación ha concluido que:

> "El aumento de la legislación y las políticas destinadas a combatir la ciberdelincuencia también ha abierto la puerta a castigar y vigilar a activistas y manifestantes en muchos países

[12] OEA. Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética. Anexo A, pág. 3. Disponible en: http://www.oas.org/juridico/english/cyb_pry_estrategia.pdf

[13] OEA. Tercera Reunión del Grupo de Expertos Gubernamentales en Materia de Delito Cibernético, OEA/Ser.K/XXXIV, CIBER-III/doc.4/03).8 y OEA. Estrategia Interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética. Anexo A.

[14]OEA. La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. OEA/Ser.D/XXV.25, pág. 50. Disponible en: https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf

> del mundo. Aunque el papel que la tecnología puede desempeñar en la promoción del terrorismo, la incitación a la violencia y la manipulación de las elecciones es una preocupación genuina y seria a nivel mundial, estas amenazas se utilizan a menudo como pretexto para hacer frente a la nueva sociedad civil digital"[15].

Lo anterior ha venido en aumento en América Latina, pues a raíz de la proliferación de información relacionada con la pandemia y en medio de protestas, los Estados se han enfocado en reglamentar los discursos expresados en línea a partir de la persecución de las voces críticas, desde un enfoque criminalizador y punitivo[16].

De esta manera, este módulo brindará una descripción general sobre la categorización del cibercrimen en los países de Latinoamérica y el Caribe y cómo, a partir de la jurisprudencia, se han consolidado estrategias efectivas de investigación a partir de la evidencia digital que permiten adecuar las conductas ilícitas ante el avance de las nuevas tecnologías. Por otro lado, permitirá comprender la aplicación adecuada del riesgo de género en la esfera digital y cuál es la respuesta estatal frente a los discursos en línea desde las leyes del cibercrimen.

¿QUÉ ES UN CIBERCRIMEN?

Pese a que no existe un consenso global sobre lo que se considera como cibercrimen, se ha tratado de acotar el término dependiendo del propósito para el cual es utilizado. Por un lado, puede referirse a la comisión de un delito en contra de la integridad, confidencialidad y disponibilidad de la información contenida en sistemas informáticos, de redes o de datos[17] o bien, a los actos que afecten la información personal y financiera causando daño o exigiendo una contraprestación[18]

Esta propuesta se deriva de los fines definidos por el Convenio sobre la Ciberdelincuencia (Convenio de Budapest)[19], los cuales son: i) la prevención de actos atentatorios de los sistemas, redes y de datos; ii) asegurar la incriminación de dichos comportamientos y iii) atribución de poderes para detectar, investigar y perseguir penalmente estos delitos. A su vez, se toma en consideración la lucha contra el cibercrimen, el racismo y la xenofobia, a través del Protocolo Adicional No. 189 al convenio de ciberdelincuencia[20].

Del mismo modo, en el escenario internacional se ha destacado que los Estados deben hacer una diferenciación entre políticas de ciberseguridad y esfuerzos para combatir la ciberdelincuencia. Si

[15]Naciones Unidas. Informe sobre los derechos a la libertad de reunión pacífica y asociación: la era digital. A/HRC/41/41. 17 de mayo de 2019. Antecedentes y Resumen, párr. 3. Disponible en: https://www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/DigitalAge.aspx

[16] CIDH. Comunicado de Prensa R78/20. CIDH y su RELE expresan preocupación por las restricciones a la libertad de expresión y el acceso a la información en la respuesta de Estados a la pandemia del COVID-19. 18 de abril de 2020. *Véase también* CIDH. Observaciones y Recomendaciones Visita de Trabajo a Colombia. Junio de 2021.

[17]Consejo de Europa. Convenio sobre Ciberdelincuencia (Convenio de Budapest). STE 185.

[18] UNODC. Comprehensive Study on Cybercrime. Febrero de 2013, pág. 17. Disponible en: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[19] En las Américas, solo 8 países han ratificado el Convenio sobre la Ciberdelincuencia (Convenio de Budapest): Argentina, Chile, Colombia, Costa Rica, Panamá, Paraguay, Perú y República Dominicana.

[20] Mientras que, de Las Américas, únicamente el Estado de Paraguay ha ratificado el Protocolo Adicional al Convenio de Ciberdelincuencia en 2018.

bien cada política termina entrelazada entre sí, los Estados deben crear una estrategia nacional de ciberseguridad que incluya mecanismos de prevención contra la ciberdelincuencia, la competencia de los órganos judiciales en estos asuntos y la promoción de las medidas de sensibilización con la sociedad[21].

De cara a las amenazas cibernéticas que ha enfrentado la región de las Américas, el monitoreo de las soluciones digitales a nivel interamericano ha cobrado mayor relevancia en los últimos 10 años. La Comisión Interamericana de Derechos Humanos (en adelante CIDH), a través de sus informes ha analizado la relación de los derechos humanos, específicamente, con las políticas de ciberseguridad[22]. Al respecto, concluye que el concepto de 'ciberseguridad' se emplea para responder a conductas criminales que se relacionan con "la seguridad de la infraestructura nacional y de las redes, a través de las cuales se provee el servicio de Internet, hasta la seguridad o la integridad de los usuarios"[23].

De esta manera, desde este organismo interamericano de protección de derechos humanos, se ha instado a los Estados a promulgar políticas y prácticas que respondan efectivamente a los riesgos en el escenario digital que enfrentan y no impliquen definiciones amplias que den lugar a tipificar nuevos delitos informáticos y a criminalizar el uso del Internet[24]. Para ello, el manejo de la ciberseguridad para estos asuntos debe propender por:

- ✓ La capacitación de los usuarios.
- ✓ La implementación de dispositivos técnicos de seguridad.
- ✓ El establecimiento de una responsabilidad compartida entre los distintos actores.
- ✓ Una sanción adecuada y efectiva de los responsables.
- ✓ La inclusión de salvaguardas legales, así como informes de transparencia y de rendición de cuentas[25].

Adicionalmente, se previó la creación de una base de datos que ayude a comprender las tendencias de los ciberdelitos[26]. En todo caso, las cuestiones que aborden la seguridad cibernética deben responder a los principios de conciencia, responsabilidad, respuesta, ética y democracia en el diseño, gestión y evaluación de la seguridad, lo cual implica el respeto por los derechos a la libertad de

[21] UNODC. Informe de la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de julio de 2020, pág. 13.
[22] RELE. Informe Anual de la Comisión Interamericana de Derechos Humanos. OEA/Ser.L/V/II Doc.28. 30 de marzo de 2021 y CIDH. Estándares para una Internet libre y segura. OEA/Ser.L/V/II. CIDH/RELE/INF.17/17. 15 de marzo de 2017.
[23] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión, Capítulo IV. Libertad de Expresión e Internet. OEA/Ser.L/V/II.149, 2013, párr. 118.
[24] Ibíd., párr. 119.
[25] CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión, Capítulo IV. Libertad de Expresión e Internet. OEA/Ser.L/V/II.149, 2013.
[26] UNODC. Informe de la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de julio de 2020, pág. 13.

pensamiento y expresión, al libre flujo de información, a la confidencialidad y protección de la información y de los datos personales[27].

Finalmente, para prevenir y responder al delito cibernético, los Estados han considerado, además, las cuestiones que reflejan la violencia contra las mujeres y niñas en línea[28] así como prestar especial atención a la propagación de discursos de odio y el extremismo[29]. Frente a la primera de ellas, tanto la Organización de las Naciones Unidas como la Organización de los Estados Americanos, han concluido que las varias formas de violencia contra las mujeres y niñas persisten y se exacerban cuando median las tecnologías de manera que están surgiendo nuevas formas de sexismo y misoginia online[30].

TIPOS DE CIBERCRÍMENES EN LATINOAMÉRICA Y EL CARIBE

a. Acceso ilegal a un sistema informático y a datos informáticos

A menudo, los actos que atentan contra la confidencialidad, integridad y disponibilidad de la información afrontan vacíos legales al interior de los Estados que inciden, así mismo, en la falta de conciencia y conocimiento sobre estas vulnerabilidades. Al respecto, Naciones Unidas ha indicado que es necesario que los Estados revisen y actualicen sus leyes en aras de responder ante estos nuevos delitos[31]. En América Latina y el Caribe, la legislación sustantiva sobre estas temáticas indica que el 87% de los países miembros de la OEA tipifican el delito de acceso ilícito a un sistema/datos informáticos, mientras que el 75% contemplan los ataques a la integridad de los mismos[32].

En el Caso No. CCC 51772/2011/T01, el Tribunal Oral Penal No. 18 de Argentina analizó los hechos en los que el imputado accedió al usuario y contraseña bancaria de la víctima a través de una manipulación indebida de datos informáticos y realizó una transferencia por una alta suma de dinero a un tercero. La valoración del Tribunal supuso la recopilación de datos a través de procedimientos de investigación sobre computadores y testimonios en los que se concluyó que el acceso operó en virtud de una transacción realizada desde México con apoyo de la Firma a la que trabajaba, ya que contaban herramientas y software que requerían de usuarios y contraseñas.

El Tribunal, por su parte, determinó que así la transferencia se haya efectuado desde una dirección IP ubicada en México, la maniobra denunciada efectivamente se cometió, pues, "de acuerdo a la nueva tecnología de que dispone cualquier persona con conocimientos de informática puede operar

[27] Naciones Unidas. Resolución 57/239 sobre los elementos para la Creación de una Cultura Mundial de Seguridad Cibernética para Sistemas y Redes de Información. Diciembre de 2002, pág. 3.
[28] Naciones Unidas. Recomendación General No. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19. CEDAW/C/GC/35. 26 de julio de 2017.
[29] UNODC. Informe de la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de julio de 2020, pág. 15.
[30] OEA. La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. OEA/Ser.D/XXV.25.
[31] Naciones Unidas. Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. A/74/130. 30 de julio de 2019, párr. 47b. Disponible en: https://www.unodc.org/documents/Cybercrime/SG_report/V1908185_S.pdf
[32]OEA. Departamento de Cooperación jurídica. Portal Interamericano de Delitos Cibernéticos. Disponible en: http://www.oas.org/es/sla/dlc/cyber-es/estado-americas.asp

un "IP" situado en otro país desde la República Argentina, incluso, mediante tutoriales en Internet que brindan instrucciones para navegar con un IP de otro país sino también para hacerlo en forma anónima"[33]. De esta manera, encontró responsable al imputado.

Este tipo de casos de manipulación informática han permitido, por ejemplo, que en países como Argentina, se avance sustancialmente en las Unidades Fiscales Especializadas en Ciberdelincuencia[34] así como se establezcan protocolos que busquen guiar las prácticas de investigación en este tipo de delitos como el "Protocolo General de Actuación para las Fuerzas Policiales y de Seguridad en la Investigación y Proceso de Recolección de Pruebas en Ciberdelitos"[35]. Brasil, por su parte, tiene delegaciones especializadas sobre ciberdelitos por cada Estado[36], en cumplimiento de la Ley 12.737/12 sobre la tipificación penal de los delitos informáticos. Por último, se han implementado planes orientados específicamente a alertar sobre las nuevas modalidades de ciberamenazas y a investigar los delitos que han sido 'ciber asistidos' en aras de responder efectivamente a esta modalidad de cibercrimen[37].

Otro evento puede ocurrir, por ejemplo, cuando a través del uso de la informática, se vulnera la protección de la información y de los datos y con ello, se tipifica el delito de violación de datos personales, de acuerdo con lo previsto en la Ley 1273 de 2009 de Colombia. Sin embargo, este delito tiene un impacto diferenciado en los periodistas.

De un lado, es claro que para su configuración, se requiere de "una intención de perseguir un provecho para sí o un tercero y que el autor no se encuentre autorizado para acceder a la información"[38], pero el contexto en el que se ha desarrollado la actividad periodística en Colombia en los últimos años, se encuentra demarcado por el uso de facultades legales del Estado para acudir a perfilamientos de periodistas, como los denunciados por Revista Semana en 2020[39]. En ese sentido, los aspectos típicos de estos delitos informáticos, deben analizarse con extremo cuidado por el riesgo que suponen frente a ciertos grupos de interés constitucional.

La Corte Suprema de Justicia analizó una solicitud de absolución en la que se alegó que i) un fiscal acusado por el delito de violación de datos personales sí estaba facultado para acceder a tales datos, ya que ii) la información no constituía un dato privado. Frente a ello, la Corte enfatizó que los funcionarios públicos pueden "acceder a información privilegiada en las bases de datos, *siempre que su actuación estuviera guiada por un interés funcional por causa del debido proceso*"[40]. Además, aclaró que el delito de violación de datos personales, no requiere que la información sea privada o

---

[33] Argentina. Cámara Federal de Casación Penal. Sala III. Causa No. CCC 51772/2011/TOI/CFC1, pág. 6.
[34] Argentina. Ministerio Público Fiscal. Resolución No. 3744/2015.
[35] Argentina. Ministerio de Justicia y Derechos Humanos. Resolución No. 234 de 2016.
[36] Safer Net. Delegacias Cibercrimes. Crimes Na Web. Disponible en: https://new.safernet.org.br/content/delegacias-cibercrimes
[37] Argentina. Ministerio de Seguridad. Resolución No. 977 de 2019.
[38] Colombia. Corte Suprema de Justicia. Sentencia 36208 de 16 de mayo de 2012. Sala Penal. Magistrado Ponente: Augusto Ibáñez Gumán, pág. 16.
[39] Colombia. Revista Semana. Informe Especial Las Carpetas Secretas. 1 de mayo de 2020. https://www.semana.com/nacion/articulo/espionaje-del-ejercito-nacional-las-carpetas-secretas-investigacion-semana/667616/ *Véase también* Revista Semana. Chuzadas sin Cuartel. 13 de mayo de 2020, en: https://www.semana.com/nacion/articulo/chuzadas-por-que-se-retiro-el-general-nicacio-martinez-del-ejercito/647810/
[40] Colombia. Corte Suprema de Justicia. Sentencia 36208 de 16 de mayo de 2012. Sala Penal. Magistrado Ponente: Augusto Ibáñez Gumán, pág. 16.

que se acredite si fue transmitida pues el reproche se realiza sobre el acceso a información personal con un interés distinto al de sus funciones[41].

b. Fraude informático

Ahora, existen otros actos que se relacionan con la informática a partir de una asociación criminal que busca un beneficio económico. El fraude cibernético o informático es aquel que utiliza plataformas de Internet o dispositivos electrónicos con el objetivo de i) acceder a información confidencial y/o ii) interceptar una transmisión electrónica para alterar, borrar, sin autorización, los datos almacenados o reescribir incluso códigos de software[42]. En la región se conocen iniciativas legislativas que tipifican el fraude informático. Según datos de la OEA, el 94% de los países miembros de América Latina y el Caribe contienen dicha reglamentación[43].

A través de la Ley 19.223 Chile tipifica los delitos informáticos y establece tipos penales tales como la sustracción de datos contenidos en sistemas de información, el espionaje informático y el sabotaje informático. Por otro lado, la Ley 20.009 contempla los delitos relacionados con el uso malicioso o apoderamiento de tarjetas de crédito. Frente a esto, en Chile, se registró un caso sucesivo de fraude en clientes de distintas entidades financieras entre 2014 y 2018.

Caso Zares en la Web v. Chile

En este caso, el acusado buscó transferir los fondos a las cuentas de una organización criminal con una estructura jerárquica que incluía a cabecillas, receptores y mandatarios; estos últimos encargados de implementar medidas para incautar información haciendo uso del Internet. El caso es comúnmente conocido como "Zares en la web" y se basó en el robo de información bancaria de los clientes a partir de las bases de datos de la "Deep web"[44].

En este caso, el Poder Judicial acreditó la existencia de 81 víctimas, entre particulares y pequeñas empresas, y condenó al máximo cabecilla por los delitos de asociación ilícita, fraude y lavado de activos, según la Ley 19.223, entre otros. En su análisis, el Juzgado 11 de Garantía de Santiago acreditó que se utilizó un engaño a partir de conocimientos en temas computacionales y accedió mediante la Internet de forma fraudulenta a información personal, como contraseñas. En sus términos, "los imputados al obtener la información personal, bancaria, claves secretas y al efectuar diversas maniobras destinadas a traspasar las medidas de seguridad y de control que tanto los clientes como las entidades bancarias utilizaban, efectuaron diversos traspasos fraudulentos de fondos de diversas cuentas corrientes, falseando a la verdad (…)"[45].

[41] Ibídem.
[42] Cornell Law School. Fraude cibernético e informático. Disponible en: https://www.law.cornell.edu/wex/es/fraude_cibern%C3%A9tico_e_inform%C3%A1tico
[43] OEA. Departamento de Cooperación jurídica. Portal Interamericano de Delitos Cibernéticos. Legislación Sustantiva. Disponible en: http://www.oas.org/es/sla/dlc/cyber-es/estado-americas.asp
[44] UNODC. Base de datos de jurisprudencia. Caso Zares de la Web c. Chile. https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/chl/2020/zares_de_la_web.html?lng=en&tmpl=sherloc
[45] Chile Poder Judicial. R.U.C.N No. 1700623543-3. T.I.T.N. No. 10355-2017. Imputado: Marco Simón Fernando Almonacid Marchant. Delito: estafa, asociación ilícita y lavado de activos.

En relación con el segundo aspecto que se deriva del fraude, el cual es interceptar una transmisión electrónica para alterar, borrar, sin autorización, los datos almacenados, en un caso ocurrido en República Dominicana, se elevaron cargos por la comisión de los "delitos de alta tecnología" en contra de la Empresa Nacional de Teléfonos del país. Esto, por cuanto se denunció el uso sospechoso de líneas de teléfono prepagadas que luego fueron convertidas ilegalmente en líneas postpago para realizar llamadas a destinos internacionales a través de una interferencia ilegal en la plataforma para evitar el pago[46].

En este caso, el Segundo Tribunal Colegiado de la Cámara Penal del Juzgado de Primera Instancia calificó jurídicamente los hechos como fraude electrónico, a la luz de lo previsto en el Código Penal y la Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología y su responsabilidad quedó acreditada por cuanto atentó contra un bien jurídico ajeno y que es protegido por el Estado, como la Compañía Dominicana de teléfonos, a partir del uso ilegal de programas para acceder a un sistema electrónico, ofrecer servicios sin pagarlos a los proveedores y comercializar de forma no autorizada bienes y servicios a través de Internet empleando dispositivos fraudulentos atentando contra las Telecomunicaciones del Estado[47].

c. Producción, distribución, posesión de pornografía infantil- Abuso infantil en línea

El uso de las tecnologías, al mismo tiempo, ha repercutido en los derechos de los niños, niñas y adolescentes. En particular, el uso de tecnologías de la información y telecomunicaciones, tiene incidencia sobre la facilidad de la comisión de actos delictivos en el escenario digital[48], lo cual incluye la explotación sexual infantil, el abuso infantil en línea y la producción, distribución, ofrecimiento y consumo material de tal abuso en línea y fuera de línea [49]. Ante la persistencia y nuevas formas de explotación sexual de niños, sobre todo en línea, en todas las regiones del mundo, una de las mayores problemáticas identificadas es la necesidad de establecer marcos jurídicos claros que tipifiquen explícita y completamente como delito la explotación sexual infantil a la luz del Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.

Sumado a lo anterior, las tecnologías tienen, además, un impacto diferenciado en mujeres sobre todo cuando ejercen una labor de interés público como el periodismo o la defensa de los derechos

[46] UNODC. Base de datos de jurisprudencia. Caso Proceso No. 058-13-00719 c. República Dominicana. https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/dom/2015/proceso_no._058-13-00719.html?lng=en&tmpl=sherloc

[47] República Dominicana. Poder Judicial. Segundo Tribunal Colegiado de la Cámara Penal del Juzgado de Primera Instancia del Distrito Nacional. Sentencia No. 434 de 2015. Proceso No. 249-04-15-00415. Págs. 33 y 34. En: https://sherloc.unodc.org/cld/uploads/res/case-law-doc/cybercrimecrimetype/dom/proceso_no__058-13-00719_html/Sentencia_Soto_y_otros

[48] Naciones Unidas. Explotación sexual de niños y tecnologías de la información y la comunicación (TIC). https://www.ohchr.org/EN/Issues/Children/Pages/InformationCommunicationTechnologies.aspx

[49] Relatora Especial sobre la Venta de Niños, la prostitución infantil y la utilización de niños en la pornografía. Declaración en la 28 sesión del Consejo de Derechos Humanos. 11 de marzo de 2015.

humanos[50]. En relación con la actividad periodística, se ha reconocido los riesgos que enfrentan cuando se difunden fotografías sin su consentimiento acompañadas de amenazas que buscan a menudo silenciar lo que se está informando. Sobre esto, el Tribunal Europeo de Derechos Humanos conoció el caso de la violación del derecho a la privacidad y de la libertad de expresión de la periodista Khadija Ismayilova por la difusión de contenido íntimo e información confidencial como una 'campaña de intimidación' frente a las investigaciones que adelantaba[51].

Como parte de su análisis legal, el Tribunal determinó que: i) el Estado de Azerbaiyán tenía la obligación de 'disuadir' actos en los que se pueda afectar la vida privada de las personas sometidas a su jurisdicción, ii) las denuncias debieron tramitarse teniendo en cuenta la protección a periodistas y la promoción de un ambiente favorable para la participación en el debate público sin temores, y iii) reconoció el efecto 'paralizador' de las injerencias a su vida privada con su derecho a la libertad de expresión[52].

En ese escenario, a nivel regional, la Convención Interamericana para Prevenir, Sancionar y Erradicar la violencia contra la mujer (Convención Belém Do Pará) reconoce que estas son condiciones indispensables para el desarrollo pleno de la mujer en todas sus esferas, incluyendo el rechazo hacia la exhibición de la pornografía como un acto de hostigamiento que se exacerba cuando median las tecnologías[53]. De manera que la violencia en línea contra niñas, adolescentes y mujeres, para la CIDH, incluye, "actos de violencia y discriminación como, entre otros, el acoso, el grooming[54] (…) videos o clips de audio sin su consentimiento; al acceso o divulgación de sus datos privados sin su consentimiento; a la carga y difusión de fotos o videos modificados de niñas y adolescentes como material de pornografía; etc."[55].

De ahí que, para UNICEF, las nuevas tecnologías contribuyen a facilitar el acceso al material de abuso infantil con menor probabilidad de identificación de los perpetradores[56]. Por ello, le corresponde a los Estados establecer leyes y políticas claras que tipifiquen los delitos cometidos en línea y fortalezcan las investigaciones para dar con el paradero de los actores. En ese orden, en países miembros de la OEA, el 94% tipifica el delito de pornografía infantil dentro de sus legislaciones[57]. De hecho, el Mecanismo de Seguimiento de la Convención Belém Do Pará

[50] CIDH. Violencia y discriminación contra mujeres, niñas y adolescentes. OEA/Ser.L/V/II.Doc.233. 14 de noviembre de 2019. Disponible en: https://www.refworld.org.es/pdfid/5e2f37804.pdf
[51] Global Freedom of Expression. TEDH. Caso Khadija Ismayilova c. Azerbaiyán. 10 de enero de 2019. Disponible en: https://globalfreedomofexpression.columbia.edu/cases/khadija-ismayilova-v-azerbaijan/
[52] Ibídem.
[53] Naciones Unidas. Recomendación General No. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19. CEDAW/C/GC/35. 26 de julio de 2017.
[54] UNICEF. Guía de Sensibilización sobre Conveniencia Digital, pág. 20. "Se denomina grooming a la situación en que un adulto acosa sexualmente a un niño o niña mediante el uso de las TIC. Los perpetradores de este delito suelen generar un perfil falso en una red social, sala de chat, foro, videojuego u otro, en donde se hacen pasar por un chico o una chica y entablan una relación de amistad y confianza con el niño o niña que quieren acosar". Disponible en: https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf
[55] CIDH. Violencia y discriminación contra mujeres, niñas y adolescentes. OEA/Ser.L/V/II.Doc.233. 14 de noviembre de 2019. Disponible en: https://www.refworld.org.es/pdfid/5e2f37804.pdf
[56] UNICEF. Estado Mundial de la infancia: Niños en un mundo digital. 2017, párr. 76 https://www.unicef.org/colombia/media/486/file/Estado%20Mundial%20de%20la%20Infancia.pdf
[57] OEA. Departamento de Cooperación jurídica. Portal Interamericano de Delitos Cibernéticos. Legislación Sustantiva. Disponible en: http://www.oas.org/es/sla/dlc/cyber-es/estado-americas.asp

(MESECVI) ha destacado las legislaciones de América Latina y el Caribe que contemplan como delitos la pornografía[58].

En el Caso No. 139-1U-2018 de El Salvador, el Tribunal Segundo de Sentencia de Santa Tecla decidió asumir conocimiento de la comisión del delito de adquisición o posesión de material pornográfico de niñas, niños y adolescentes por una red transnacional[59].

Este caso es relevante desde la etapa de recolección del material probatorio, por cuanto de un lado, registraron e incautaron todos los equipos de almacenamiento masivo que se encontraban en los inmuebles relacionados en el proceso siempre que tuvieran material pornográfico. Por otra parte, realizaron peritajes "de campo" por medio de los cuales identificaron científicamente a las personas que descargaron este contenido"[60].

Frente al *modus operandi*, la jueza destacó que "ya no solamente sea en búsquedas aisladas en la Deep web para obtener este material pornográfico infantil, ahora se pueden formar grupos en diversas páginas web o en redes sociales, para obtenerlo y compartirlo"[61], ya que se comprobó que en este caso las personas utilizaron un grupo de WhatsApp para difundir el material.

Pero además, frente a la responsabilidad penal de las personas involucradas, la jueza señaló que cada imagen contiene un dato propio o metadato, de tal suerte que permite el rastreo de: "cuando fue creada, por quien fue enviada, en qué momento se descargó y demás elementos que pudieran profundizar en si existía difusión o distribución de este material con alto contenido de pornografía infantil por parte del procesado". De esta manera, puso de presente la necesidad de revelar completamente la red criminal de este tipo penal, incluyendo la identificación del consumidor final y otras acciones que impactan el seno de la sociedad valiéndose de la misma tecnología para identificarlos.

[58] OEA. Mecanismo de Seguimiento Convención Belém Do Pará. Recomendación General del Comité de Expertas del MESCVI (No. 3) La figura del consentimiento en casos de violencia contra las mujeres por razones de género. OEA/Ser.L/II/7.10 MESECVI/CEVI/doc.267/21. 7 de diciembre de 2021, pág. 20. Disponible en: https://www.oas.org/es/mesecvi/docs/MESECVI_CEVI_doc.267_21.ESP.RecomendacionGeneralConsentimientoSexual.XVIII%20CEVI.pdf

[59] UNODC. Base de datos de jurisprudencia. Caso No. 139-1U-208 c. El Salvador. Disponible en: https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/slv/2018/139-1u-2018.html?lng=en&tmpl=sherloc

[60] El Salvador. Tribunal Segundo de Sentencia de Santa Tecla. Departamento de la Libertad. 28 de septiembre de 2018. Sentencia no. 139-1U-2018, pág. 4.

[61] El Salvador. Tribunal Segundo de Sentencia de Santa Tecla. Departamento de la Libertad. 28 de septiembre de 2018. Sentencia No. 139-1U-2018, Fundamento del Fallo No. 24.

Caso Operación R-INO v. Costa Rica

Otra dimensión de la pornografía infantil resulta de la captación de víctimas bajo engaño. En Costa Rica, a través del Caso "Operación R-INO", se tuvo conocimiento de una agencia de modelos que realizaba castings mediante redes sociales y en las audiciones con menores de edad, los fotógrafos produjeron material de pornografía para ser distribuidos en sitios web y la Deep web. La relevancia de este caso radica en que, para ocultar sus huellas digitales, la organización criminal restringió el contenido a las direcciones IP públicas de Costa Rica de tal manera que solo se pudiera acceder al contenido desde el exterior[62].

Este caso denota, así mismo, la existencia de técnicas especiales de investigación electrónica y otras formas de vigilancia, que dieron con el dominio de sitios web registrados en 3 países distintos, lo que permitió la identificación de cada uno de los integrantes de la organización transnacional. Pero, además, es un caso fundamental porque, por primera vez, Costa Rica realizó allanamientos a un sitio web con fundamento en una orden judicial. "Se accedió a los sitios web mediante TOR, debido al bloqueo geográfico. A través del "agente encubierto", se creó una cuenta de correo electrónico ficticia para acceder a estas páginas. Una gran cantidad de material de abuso sexual de las víctimas fue descargado como evidencia del caso"[63].

Finalmente, a raíz de lo sucedido en la pandemia por COVID-19 y la proliferación de las plataformas digitales para comunicarse, como Zoom, el Tribunal de Apelaciones del Tercer Circuito de los Estados Unidos en Pensilvania analizó el Caso No. 19-2424 y 19-2932, el cual involucra a dos sujetos que usaron videoconferencias en Zoom para "ver, solicitar, recibir, distribuir y facilitar la recepción y distribución de material de abuso sexual infantil. Dentro de Zoom, se compartió material de abuso sexual infantil pregrabado, así como transmisión en vivo de abuso sexual infantil"[64].

El esquema de la investigación, como en los casos anteriores, resultó en la efectividad del proceso judicial. Se rastrearon las direcciones IP de algunos de los usuarios de la reunión de Zoom y se recopiló evidencia electrónica a partir de la labor de un agente encubierto en virtud de la cooperación con Canadá[65]. Además, se apeló a la intervención de intermediarios como el Director Ejecutivo de Zoom, en aras de colaborar con la investigación de presuntas conductas ilícitas desarrolladas en su plataforma.

---

[62] UNODC. Base de datos de jurisprudencia. Caso Operaciòn R-INO c. Costa Rica. Disponible en: https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/cri/operacion_r-ino.html?lng=en&tmpl=sherloc

[63] Ibìdem.

[64] UNODC. Base datos de jurisprudencia. Caso Dylan Heatherly, No. 19-2424 (3d Cir. Dec. 11, 2020) and United States v. William Staples, No. 19-2932 (3d Cir. Dec. 11, 2020). Disponible en: https://sherloc.unodc.org/cld//case-law-doc/cybercrimecrimetype/usa/2020/united_states_v._dylan_heatherly_no._19-2424_3d_cir._dec._11_2020_and_united_states_v._william_staples_no._19-2932_3d_cir._dec._11_2020.html?lng=en&tmpl=sherloc

[65] United States Court Of Appeals For The Third Circuit. Nos. 19-2424 & 19-2932. United States Of America V. Dylan Heatherly, Also Known As Daniel Sotherland, Also Known As John Doe-9. Appellant In No. 19-2424. United States Of America. William Staples, Also Known As Bill Simpson, Also Known As John Doe-7, Appellant In No. 19-2932, Pág. 5. Traducción Propia.

La importancia del caso recae en que el Tribunal admitió los videoclips incautados en los dispositivos móviles de los dos sujetos como prueba de recibo y distribución del material, pese a que alegaron ser meros observadores de contenido, toda vez que fueron "esenciales para probar la conspiración tácita de la cultura de esa reunión de Zoom y el conocimiento de lo que estaban buscando los dos sujetos en la plataforma"[66].

d. Violencia de género en línea: hacia la categorización de la violencia telemática y la tipificación de delitos asociados al género en la región

La expansión de las tecnologías en la región tiene un impacto transversal en las relaciones de género. Por un lado, la Agenda 2030 destaca la necesidad de superar la brecha digital en aras de alcanzar la igualdad de género y, por el otro, eliminar todas las formas de violencia contra la mujer tanto online como offline. A nivel internacional, se ha reconocido que la violencia en línea en contra de mujeres y niñas es cada vez más frecuente y se extiende al espacio digital de las redes sociales como Twitter, Facebook, Instagram, YouTube, entre otros, de modo que los Estados deben avanzar en el reconocimiento legal de estas formas "múltiples, interrelacionadas y recurrentes de violencia por razón de género contra la mujer"[67].

Según la UNESCO, en una encuesta realizada en el año 2020, cerca del 73% de las más de 900 periodistas encuestadas sufrieron de violencia en línea, de las cuales 714 se identificaron como mujeres[68]. La violencia que frecuentemente experimentan trae consigo impactos diferenciados sobre todo en la salud mental, de tal suerte que el 12% de ellas buscó ayuda médica y psicológica. Por otro lado, los temas periodísticos relacionados con estas agresiones en línea fueron el género (47%), política y elecciones (44%) y derechos humanos y política social (31%)[69].

Dentro del ámbito de las Naciones Unidas, la Relatoría Especial sobre la Violencia contra la Mujer señaló su preocupación ante el incremento de violencias en línea y concluyó que este tipo de violencias se constituyen en violaciones particulares de derechos humanos de las mujeres[70]. Sumado a que esta violencia en línea afecta de forma desproporcionada a las mujeres periodistas y trabajadoras de medios de comunicación[71].

---

[66] United States Court Of Appeals For The Third Circuit. Nos. 19-2424 & 19-2932. United States Of America V. Dylan Heatherly, Also Known As Daniel Sotherland, Also Known As John Doe-9. Appellant In No. 19-2424. United States Of America. William Staples, Also Known As Bill Simpson, Also Known As John Doe-7, Appellant In No. 19-2932, Pág. 36. Traducción Propia.

[67] Naciones Unidas. Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. 18 de junio de 2018, párr. 12.

[68] UNESCO. The Chilling: Global trends in online violence against women journalist. Abril de 2021. Disponible en https://en.unesco.org/sites/default/files/the-chilling.pdf

[69] Ibídem.

[70] Naciones Unidas. Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. 18 de junio de 2018.

[71] Consejo de Derechos Humanos. Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. 18 de junio de 2018, párr. 29.

Este tipo de violencias incluye "el monitoreo y acecho, la publicación de datos personales, trolling, desprestigio, la difamación o la descalificación y el odio viral"[72] y tienen como objetivo intimidar, controlar, acallar a las mujeres que cubren temas de interés público[73]. Por ello, es cada vez más frecuente que las mujeres periodistas decidan autocensurarse o en casos extremos abandonar su profesión[74]. En otras circunstancias, las mujeres cambian de nombre, usan seudónimos o simplemente desactivan sus cuentas[75].

Para ejemplificar lo anterior, en el caso colombiano, una investigación realizada por la Universidad de los Andes y la iniciativa No es hora de callar, evidenció que el 37% de las mujeres periodistas encuestadas fueron obligadas a abandonar sus espacios de trabajo, el 24% a cambiar sus temas de cubrimiento y el 47% a abandonar ciertas fuentes, con ocasión de esta violencia en línea[76]. Al mismo tiempo, la Fundación Karisma y la Red Colombiana de Periodistas señalaron que cerca del 77.1% reciben comentarios violentos a través de redes sociales, de los cuales el 22.7% son humillaciones, el 18.3% busca silenciarlas y el 10.4% son campañas que apuntan a su descrédito[77].

En la esfera interamericana, por su parte, la Relatoría para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos se enfocó en decantar la violencia en el ámbito de las nuevas tecnologías y su riesgo concreto sobre niños, niñas y adolescentes. Además, determinó que la violencia contra las mujeres en Internet es "una violencia por razones de género"[78].

Sobre el particular de la violencia en línea contra mujeres periodistas, manifestó que esta afecta de forma directa su visibilidad y participación en el escenario público, máxime cuando no existen avances sustanciales en la investigación, juzgamiento y sanción de estas conductas que alientan a la impunidad[79]. Sin embargo, este efecto se exacerba cuando los perpetradores de la violencia usan cuentas anónimas[80]. Además, se reconoció que esto, al mismo tiempo, puede impactar en sus derechos a la integridad física, moral y mental[81]. De ahí la necesidad de que los Estados cuenten

[72] UNESCO. Tendencias Mundiales en libertad de expresión y desarrollo de los medios. Informe Mundial 2017-2018, p. 156.
[73] CIDH. Relatoría Especial para la Libertad de Expresión. Mujeres periodistas y libertad de expresión. OEA/SER.L/V/II CIDH/RELE/INF.20/18. 31 de octubre de 2018, párr. 47.
[74] Ferrier, Michelle. Attacks and Harassment: the impact on Female Journalists and their Reporting. International Women's Media Foundation; Troll-Busters.com. 2018.
[75] Consejo de Derechos Humanos. Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias, acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos. A/HRC/38/47. 18 de junio de 2018, párr. 29.
[76] Observatorio de la democracia y Universidad de los Andes. No es hora de callar. Violencia de género en contra de las mujeres periodistas en Colombia. 2020. Disponible en: https://obsdemocracia.org/uploads/related_file/Informe_NEHDC.pdf
[77] Red Colombiana de Periodistas con Visión de Género y Fundación Karisma. Periodistas sin Acoso. Violencias machistas contra periodistas y comunicadoras. 2021, p. 23.
[78] CIDH. Violencia y discriminación contra mujeres, niñas y adolescentes. OEA/Ser.L/V/II.Doc.233. 14 de noviembre de 2019, párr. 303. Disponible en: https://www.refworld.org.es/pdfid/5e2f37804.pdf
[79] CIDH. Relatoría Especial para la Libertad de Expresión. Mujeres periodistas y libertad de expresión. OEA/SER.L/V/II CIDH/RELE/INF.20/18. 31 de octubre de 2018, párr. 59.
[80] Consejo de Derechos Humanos. Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias. A/HRC/44/52. 6 de mayo de 2020, párr. 40.
[81] OEA. Combatir la violencia en línea contra las mujeres. Un llamado de protección, p. 8. Disponible en https://www.oas.org/es/sms/cicte/docs/20191125-ESP-White-Paper-7-VIOLENCE-AGAINST-WOMEN.pdf

con sistemas legales sólidos con capacidad presupuestal y técnica para investigar estos hechos, así como perseguir y sancionar a los responsables[82].

Por ello, en el interior de la OEA se creó una asociación entre el Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo (CICTE) y la Comisión Interamericana de Mujeres (CIM) para analizar, desde un enfoque regional, los desafíos a la seguridad digital observando las particularidades del género[83]. Como respuesta a esta violencia, los Estados por su lado han modificado sus marcos jurídicos en aras de avanzar hacia la tipificación de delitos con cierto contenido de género.

Así, por ejemplo, en países de la región como Perú, se ha avanzado en la tipificación de delitos de acoso sexual, chantaje sexual y difusión de imágenes íntimas a través del uso de las tecnologías en su Código Penal, mediante el Decreto Legislativo No. 1410 de 2018. Brasil, por su parte, promulgó la Ley 13.772 de 2018, que considera como delito la grabación y el almacenamiento no autorizado de contenidos íntimos y privados y la Ley 13.718 de 2018 que tipifica la difusión de imágenes que contengan "una escena de violación o que haga una apología o induzca a su práctica; o una escena de sexo, desnudez o pornografía sin el consentimiento de la víctima". Por otro lado, Argentina tipifica conductas relacionadas con "la difusión de imágenes o grabaciones íntimas y el hostigamiento digital"[84].

En Paraguay, la Ley 5777/16 condensó la protección integral de las mujeres contra todas las formas de violencia, incluyendo la telemática. Pese a que su definición es limitada, deja por fuera otros actos delictivos como el acoso en línea, las amenazas, abuso y explotación sexual en línea, las expresiones discriminatorias, entre otras[85].

Paraguay: violencia telemática

Este tipo de violencia se define como aquella "por medio de la cual se difunden o publican mensajes, fotografías, audios, vídeos u otros que afecten la dignidad o intimidad de las mujeres a través de las actuales tecnologías de información y comunicación, incluido el uso de estos medios para promover la cosificación, sumisión o explotación de la mujer. Se entenderá por «cosificación» a la acción de reducir a la mujer a la condición de cosa".

[82] CIDH. Relatoría Especial para la Libertad de Expresión. Mujeres periodistas y libertad de expresión. OEA/SER.L/V/II CIDH/RELE/INF.20/18. 31 de octubre de 2018, párr. 58.
[83] OEA. La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. OEA/Ser.D/XXV.25, pág. 50. Disponible en: https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf
[84] OEA. La violencia de género en línea contra las mujeres y niñas. Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta. OEA/Ser.D/XXV.25, pág. 51. Disponible en: https://www.oas.org/es/sms/cicte/docs/Manual-La-violencia-de-genero-en-linea-contra-las-mujeres-y-ninas.pdf
[85] TEDIC. Violencia de género en Internet en Paraguay. Un estudio exploratorio. Julio 2021, pág. 17. En: https://www.tedic.org/wp-content/uploads/2021/08/Violencia-Digital-TEDIC-WRO-2021-ES-v01.pdf

México, por su parte, impulsó el reconocimiento de la violencia digital en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia como aquella acción dolosa que se vale del uso de las tecnologías y que además causa "un daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia". Paralelamente, adicionó al Código Penal Federal los "delitos contra la indemnidad de privacidad de la información sexual" e incluye los supuestos de: i) quien divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual sin autorización y ii) quien videograbe, audiograbe, fotografíe, imprima o elabore, imágenes, audios o videos con contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación, o sin su autorización[86].

Es importante subrayar la situación de México. La violencia contra las mujeres y niñas en este país agudizadas por las tecnologías de la información y la comunicación (TIC), son cada vez mayores. Así, se tiene que tan solo el ciberacoso afecta a 9.4 millones de mujeres mexicanas, entre 18 y 30 años. Este, a menudo, es de índole sexual como insinuaciones del cual se tiene el porcentaje de 40.3% y fotos con contenido sexual no solicitado el 32.8%[87].

En efecto, el avance más significativo a nivel normativo se relaciona con la expedición de la "Ley Olimpia", en respuesta a la difusión de un vídeo de contenido sexual no autorizado. La ley busca "reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales" y ya ha sido replicada en 17 Estados de México.

Otro avance reciente se da en Ecuador. La Corte Constitucional emitió el fallo No. 2064-14-EP/21, en el que analizó el caso de una mujer víctima de pornografía no consentida y acreditó la violación de sus derechos a la protección de datos personales y autodeterminación informativa, a la imagen, a la honra, al buen nombre e intimidad por difundir imágenes íntimas sin consentimiento. En esta sentencia, la Corte arguyó que "en cuanto a la acción de haber exhibido las fotografías, está claro que el tipo de información que tenía la demandada en su poder, el hecho de que no tenía el consentimiento de la actora para realizar esa operación sobre el dato, así como la finalidad que persiguió la demandada al divulgar esas fotografías, además de la capacidad que tiene esta operación para producir efectos fuera del ámbito doméstico".

Por último, en aplicación de la legislación prevista para la garantía del consentimiento expreso en relación con imágenes publicadas en Internet, la Corte Suprema de la Justicia de la Nación de Argentina estudió el Caso de Mazza, Valeria Raque c. Yahoo SRL Argentina y otros, en el que Mazza demandó a los motores de búsqueda de Google inc. y Yahoo Argentina por hacer uso comercial y no autorizado de su imagen y afectar sus derechos a la imagen, nombre e intimidad a causa de su vinculación con páginas de contenido pornográfico.

En relación con la demanda, la Corte reiteró el precedente que los motores de búsqueda asociados a un contenido concreto configuran la responsabilidad cuando con el material ofrecido a los usuarios de la plataforma tiene conocimiento de un perjuicio individualizado y no adopta ninguna medida para

[86] México. Decreto por el que se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres y a una Vida libre de violencias y al Código Penal Federal. 1 de junio de 2021, art. 199.
[87] ONU Mujeres. Violencia contra mujeres y niñas en el espacio digital. Lo que es virtual también es real. En: https://mexico.unwomen.org/sites/default/files/Field%20Office%20Mexico/Documentos/Publicaciones/2020/Diciembre%202020/FactSheet%20Violencia%20digital.pdf

cesarlo. De esta forma, aseveró que "resulta responsable cuando, teniendo un conocimiento efectivo de que la actividad o la información a la que remite o recomienda [el buscador] causa un perjuicio individualizado, no actúa con diligencia para suprimir o inutilizar el enlace correspondiente". Para ello, se refirió a otros casos como "Rodríguez, María Belén y el Caso de "Gimbutas, Carolina Valeria (Fallos: 337;1174 y 340:1236)".

Finalmente, la Corte Suprema de Justicia de Colombia, a través de su sentencia No. SP4573-2019, ha determinado el alcance del 'grooming' y se deriva de "todo acto llevado a cabo por un adulto que implique crear una conexión emocional con un menor a fin de abusarlo o explotarlo sexualmente". Además, reconoció que el medio más frecuente que se utiliza es el Internet, de ahí que se introduzca el concepto de "online grooming"[88].

TENDENCIAS EMERGENTES EN LA REGIÓN: USO DEL DERECHO PENAL PARA CRIMINALIZAR LOS DISCURSOS EN LÍNEA

Sancionar la difusión de la información en línea ha sido una medida implementada por los Estados en contextos de contención social como el generado por la pandemia e incluso en medio de protestas. Sin embargo, esto tiene dos efectos particulares: por un lado, conlleva a la criminalización de los discursos expresados en línea a través del uso del derecho penal y, por el otro, genera un efecto inhibitorio frente a la difusión de ideas y críticas sobre temas de interés público[89].

En relación con la pandemia generada por COVID-19, la OMS expresó su preocupación frente a lo considerado como 'infodemia', al tratarse de "la rápida difusión de información de todo tipo, incluidos rumores, chismes e información poco fiable"[90]. Sin embargo, indicó que es necesario identificar esta información, analizarla y establecer medidas de control y mitigación.

El Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, por su parte, señaló que "los principios de legalidad y necesidad deben aplicarse a cualquier enfoque adoptado para hacer frente a la desinformación. En particular, la "desinformación" es un concepto extraordinariamente difícil de plasmar en la ley y es susceptible de dar al poder ejecutivo una facultad discrecional excesivamente amplia para determinar qué es desinformación, qué es un error y qué es la verdad"[91]. En ese sentido, puntualizó que los Estados no deben acudir al derecho penal para criminalizar la desinformación por los efectos disuasivos e inhibitorios que ello genera[92].

[88] Corte Suprema de Justicia. Sentencia SP4573-2019. M.P. Eugenio Fernández Carlier. 24 de octubre de 2019, pág. 43.
[89] RELE. Informe Anual de la Comisión Interamericana de Derechos Humanos. OEA/Ser.L/V/II Doc.28. 30 de marzo de 2021, párr. 105.
[90] OMS, Managing Epidemics, pág. 34
[91] Naciones Unidas.Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Las pandemias y la libertad de opinión y de expresión. A/HRC/44/49. 23 de abril de 2020, párr. 42.
[92] Naciones Unidas.Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. Las pandemias y la libertad de opinión y de expresión. A/HRC/44/49. 23 de abril de 2020, párr. 43.

La Comisión Interamericana expidió la Resolución 1 de 2020, la cual pone de presente que, en caso de responsabilizar la difusión de información bajo intereses de salud pública, los Estados están sometidos a los principios de legalidad, proporcionalidad y necesidad. Además, destacó la importancia de acceder a la información relacionada con estos temas, así como monitorear las acciones del gobierno.

Mientras que algunos Estados acudieron a medidas como "perturbar Internet y las leyes para censurar, castigar o restringir la difusión hasta la regulación de las plataformas de medios sociales" como respuesta a la desinformación[93], en el marco de manifestaciones sociales, el Relator sobre el derecho a la libertad a la reunión pacífica y asociación manifestó su preocupación frente a la aplicación de leyes dirigidas a responder a los crímenes en línea bajo conceptos ambiguos de lo que significa 'seguridad nacional'[94] u objetivos 'antiterroristas', de tal suerte que están acudiendo a criminalizar las actividades en línea en muchos países del mundo[95].

En el contexto regional, en el marco de la pandemia, como medidas para contrarrestar la desinformación relacionada al Covid-19, los Estados utilizaron leyes orientadas a criminalizar los discursos en línea desde la aplicación del concepto de cibercrimen. Por un lado, Nicaragua expidió la Ley Especial de Ciberdelitos, por medio de la cual se tipifica la conducta de propagar noticias falsas a través de las tecnologías de la información. De manera que se castiga a quien "publique o difunda información falsa o tergiversada"[96].

Por otro lado, en Argentina, se tuvo conocimiento del despliegue de actividades de 'ciberpatrullaje' o vigilancias masivas en redes sociales a cargo de las fuerzas de seguridad que resultaron en la apertura de casos por el delito de intimidación pública "contra personas que publicaban información sobre COVID-19 que difería de la local"[97]. Pese a que contempla el principio de no criminalización de las protestas en línea y el principio de protección de la libertad de expresión, el Protocolo General para la Prevención Policial del Delito con uso de fuentes digitales abiertas prevé facultades para analizar la comisión de conductas delictivas a través del uso de fuentes digitales de información.

Al mismo tiempo, en el marco de la emergencia sanitaria, Bolivia anunció el desarrollo de actividades de ciberpatrullaje para "detectar a las personas que en su criterio desinformen en las redes sociales" sobre el coronavirus[98].

Cabe recordar que en 2017 los mandatos especiales de ONU, CADHP, OSCE y CIDH adoptaron

[93] Naciones Unidas.Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión. La desinformación y la libertad de opinión y de expresión. A/HRC/47/25. 13 de abril de 2021, párr. 46.
[94] Naciones Unidas. Informe sobre los derechos a la libertad de reunión pacífica y asociación: la era digital. A/HRC/41/41. 17 de mayo de 2019, párr. 33. https://www.icnl.org/wp-content/uploads/A_HRC_41_41_E.pdf
[95] Ibíd., párr. 39.
[96] Nicaragua. Ley Especial de Ciberdelitos No. 1042 del 27 de octubre de 2020. Diario Oficial No. 201 del 30 de octubre de 2020, art. 30.
[97] RELE. Informe Anual de la Comisión Interamericana de Derechos Humanos. OEA/Ser.L/V/II Doc.28. 30 de marzo de 2021, párr. 17.
[98] RELE. Informe Anual de la Comisión Interamericana de Derechos Humanos. OEA/Ser.L/V/II Doc.28. 30 de marzo de 2021, párr. 108.

la Declaración Conjunta sobre la Libertad de Expresión y Noticias Falsas, Desinformación y Propaganda, la cual establece que "las prohibiciones generales de difusión de información basadas en conceptos imprecisos y ambiguos, incluidos «noticias falsas» («fake news») o «información no objetiva», son incompatibles con los estándares internacionales sobre restricciones a la libertad de expresión".

A nivel interamericano, se publicó la *Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales*, la cual analizó la imposición de responsabilidades ulteriores por la difusión de desinformación y noticias falsas y determinó que:

"Los Estados de la región, en línea con los estándares del sistema interamericano de derechos humanos, no deberían establecer nuevos tipos penales para sancionar la difusión de desinformación o de noticias falsas. Introducir tipos penales, que por la naturaleza del fenómeno serían vagos o ambiguos, podría retrotraer a la región a una lógica de criminalizar expresiones sobre funcionarios o personas involucradas en asuntos de interés público y establecer una herramienta con un fuerte efecto inhibitorio de la difusión de ideas, críticas e información por miedo a sufrir un proceso penal, lo que sería particularmente restrictivo en el contexto de la contienda electoral"[99].

Finalmente, en el marco de las manifestaciones convocadas para el 28 de abril de 2021 en Colombia, el Ministerio de Defensa, a través de sus redes sociales, comunicó la instalación de un Puesto de Mando Unificado de Ciberseguridad (PMU-Ciber) que se encargaba de realizar labores de ciberpatrullaje para "aclarar" informaciones que desacreditaban la labor de la Fuerza Pública en las protestas y para ello, clasificaban las expresiones bajo la etiqueta de falso y las criminalizaban al decir que hacían parte de 'terrorismo digital'[100]. Esto lo hacían desplegando sus capacidades en ciberseguridad de la mano con la actuación de 7 entidades del Estado encargadas de esos asuntos.

Sobre este tema en particular, la CIDH señaló esa tendencia creciente del uso de estas prácticas en los Estados de las Américas de modo que las actividades de patrullaje en línea permiten "la parametrización oficial de la expresión de quienes se manifiestan a través de redes sociales y el uso de diversas tecnologías para monitorear a periodistas, activistas, líderes sociales y políticos de algunos países de la región"[101]. Esto es problemático por cuanto puede generar un ambiente de censura y silencio de expresiones críticas y genera un efecto inhibitorio en la denuncia de actos de las autoridades[102].

[99] OEA. CIDH. RELE. Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales. Pág. 23. https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf

[100] Ministerio de Defensa Nacional. Las #NoticiasFalsas buscan propagar el caos. (8 de mayo de 2021).

[101] RELE. Informe Anual de la Comisión Interamericana de Derechos Humanos. OEA/Ser.L/V/II Doc.28. 30 de marzo de 2021, párr. 408.

[102] Asociación para el Progreso de las Comunicaciones (APC). Ley Especial de Ciberdelitos en Nicaragua promueve la censura y la criminalización del uso cotidiano de las tecnologías. Disponible en:

CONCLUSIONES

La falta de un consenso global sobre el término 'cibercrimen' y la ausencia de una definición de las conductas calificadas como tal, deja una amplitud en la definición jurídica y acciones de cada Estado para contrarrestar los nuevos fenómenos digitales que emergen. A ello se suma la tendencia que muchos Estados están recurriendo a las leyes de cibercrímenes para criminalizar los discursos en línea, por ejemplo. Si bien existe un avance en la tipificación de delitos que se cometen en el escenario digital con una dimensión de género, se hace necesario que a partir de la cooperación interestatal y con la OEA, los Estados de la región avancen en una reglamentación conjunta que permita responder de forma adecuada a las conductas que usualmente se cometen con impacto transnacional.

https://www.apc.org/es/pubs/ley-especial-de-ciberdelitos-en-nicaragua-promueve-la-censura-y-la-criminalizacion-del-uso