Capítulo 5

Los delitos informáticos y la problemática trasnacional: el caso colombiano*

DOI: https://doi.org/10.25062/9786287602120.05

Paola Alexandra Sierra-Zamora
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Tania Lucia Fonseca-Ortiz
Ana Mayerli Martínez Gil
Universidad Católica de Colombia

Resumen: Con el propósito de determinar las medidas de protección normativas y jurisprudenciales que ha proporcionado el Estado colombiano frente a los delitos informáticos, este capítulo por medio de una investigación cualitativa analiza la génesis de la criminalidad cibernética, así como la transformación que en la actualidad se da en el intercambio de información, dado que, el fenómeno no se limita a un territorio especifico, obligando a que su caracterización tenga un relacionamiento transnacional. Como resultado, el manejo que el sistema judicial interno y el latinoamericano le dan a la actividad delincuencial que trasciende el mundo tridimensional media una atención especial a los derechos de los sujetos involucrados y el amparo efectivo del tratamiento de la información, requiriendo herramientas como la cooperación internacional que permita una atención priorizada y coherente a los habitantes del territorio nacional.

Palabras clave: Colombia; cibercrimen; riesgos; seguridad; trasnacional.

* Este capítulo presenta los resultados colaborativos dos proyectos de investigación: 1) "La guerra asimétrica, híbrida e irrestricta: Retos, amenazas y desafíos para los Estados, la seguridad y defensa regional" del grupo de investigación "Masa Crítica" de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado en A1 por Minciencias y con código de registro COL0123247, y 2) "Retos y desafíos para el constitucionalismo transformador, el diálogo entre jueces y el derecho internacional" del grupo de investigación "Persona, Instituciones y Exigencias de Justicia" de la Universidad Católica de Colombia, categorizado en A1 por Minciencias y con código de registro COL0123247. Los puntos de vista pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Paola Alexandra Sierra-Zamora
Posdoctora internacional en Nuevas Tecnologías y Derecho. PhD Internacional (*Cum laude*) y magíster en Derechos Humanos, Democracia y Justicia Internacional, Universitat de Valéncia, España. Abogada, Universidad Católica de Colombia. Investigadora asociada y par evaluador categorizada por MinCiencias. https://orcid.org/0000-0002-3146-7418 – Contacto: paola.sierraz@esdeg.edu.co

Tania Lucia Fonseca-Ortiz
Magíster (c) en Educación Inclusiva e Intercultural, Universidad El Bosque. Abogada titulada con honores, Universidad Católica de Colombia. Joven Investigadora del Grupo de Investigación "Persona, Instituciones y Exigencias de justicia" de la Universidad Católica de Colombia. https://orcid.org/0000-0001-5089-3562 - Contacto: tlfonseca64@ucatolica.edu.co

Ana Mayerli Martínez Gil
Estudiante de Derecho, Universidad Católica de Colombia. Auxiliar de Investigación del semillero de investigación Observatorio de justicia constitucional y de Derechos Humanos, del grupo de investigación "Persona, instituciones y exigencias de justicia" de la Universidad Católica de Colombia. https://orcid.org/0000-0003-1053-1502 - Contacto: ammartinez14@ucatolica.edu.co

Citación APA: Sierra-Zamora, P. A., Fonseca-Ortiz, T. L. & Martínez Gil, A. M. (2022). Los delitos informáticos y la problemática trasnacional: el caso colombiano. En P. A. Sierra-Zamora, T. L. Fonseca-Ortiz, & F. Coronado-Camero (Eds.), *De los delitos transnacionales, las Fuerzas Armadas y el tratamiento jurídico de la seguridad y defensa nacionales* (pp. 157-177). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602120.05

De los delitos transnacionales, las Fuerzas Armadas y el tratamiento jurídico de la seguridad y defensa nacionales
ISBN impreso: 978-628-7602-11-3
ISBN digital: 978-628-7602-12-0
DOI: https://doi.org/10.25062/9786287602120
Colección Estrategia, Geopolítica y Cultura
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2022

Introducción

La tecnología es un conjunto de saberes que permite fabricar objetos y modificar el medio ambiente para satisfacer las necesidades y los deseos humanos; así mismo, ha tenido una evolución con el pasar del tiempo y se ha convertido en una herramienta técnica que ayuda al desarrollo de diversas actividades económicas, sociales, educativas y culturales. La tecnología de operación es uno de tantos tipos que existen y que tienen como propósito práctico mantener ciertos hábitos que se observan en el común, como las redes sociales y las aplicaciones que gestionan actividades de aprendizaje o enseñanza; es decir que son medios por los cuales se usa el internet, que generan ayuda y son de gran utilidad para la humanidad.

Ahora bien, aparte de traer beneficios para la sociedad, también juega en contra de ella; por ejemplo, el riesgo que representa dejar la información personal que podría generar una vulnerabilidad a la integridad de las personas, las acciones ilegales, el acceso a información poco fiable o falsa, la estafa, los robos, los delitos de propiedad intelectual, la suplantación de identidad y el hurto a cuentas bancarias y tarjetas de créditos. En tal sentido, se busca la protección personal que ha sido expuesta en el mundo informático (Salvadori, 2010, p. 61).

Aquellas actividades ilegales que han afectado a diferentes países (como Colombia, Alemania, EE. UU., Francia, Chile y España) son consideradas como delitos informáticos trasnacionales. El nuevo riesgo, generado por el uso delictivo de la tecnología informática, tiene una alta potencialidad lesiva para la sociedad actual, cuya dependencia del computador la hace sumamente vulnerable. Ello relacionado con el carácter global o transnacional de la criminalidad organizada, asociado a los efectos de la globalización sobre los límites estatales impuestos para la realización de operaciones económicas con el exterior que

han fomentado su aumento, fluidez y que han derivado en una tendencia hacia la homogeneización de los mercados (Gutiérrez, 1991, p. 24).

Con el propósito de analizar, identificar, reconocer y mostrar el impacto social que ha generado esta problemática en Colombia, se ha planteado el siguiente interrogante: ¿Qué medida de protección y seguridad ha proporcionado el Estado colombiano frente a los delitos informáticos? Lo anterior se responderá a lo largo de este capítulo, mediante una investigación de carácter analítico, a fin de estudiar todos los aspectos de los delitos informáticos, lo cual requerirá detallar los elementos básicos que componen la informática para conocer los aspectos sociales y la forma en la cual está involucrada la sociedad misma (por medio de estadísticas y de recopilación de información).

A lo largo de esta investigación se desarrollarán cuatro ejes estratégicos para la solución del problema de investigación. En primera instancia, se buscará tener claridad del concepto 'delito informático' y sus antecedentes históricos, a fin de conocer su evolución y su intervención en la sociedad. En segunda instancia, se pretenderá conocer las razones principales que han llevado a cometer delitos informáticos, con el objetivo de reconocer las modalidades en las que se opera y la forma de hacerlo. En tercera instancia, se observará el derecho comparado de Colombia y Chile, con la intención de entender la normatividad del derecho penal de estos dos países para poder comparar los aspectos jurídicos netos de nuestra nación, frente a la internacional. En cuarta, y última, instancia, se intentará identificar de qué manera ha existido una vulneración de los derechos fundamentales de la sociedad mediante la comisión de los delitos y la manipulación informática, con el fin de reconocer a las víctimas afectadas.

Conceptualización y antecedentes históricos de los delitos informáticos

Ha resultado difícil encontrar una definición o una conceptualización con respecto de qué son los delitos informáticos; por lo tanto, diferentes especialistas del tema han compartido sus ideas para crear uno que se asemeje más. Según Lima (1984), existen dos modos de comprender el delito informático. El primero, es en un sentido amplio, mediante el cual se afirma que hace referencia a cualquier conducta criminógena o criminal que hace uso de la tecnología para su realización (ya sea como método, medio o fin). El segundo, es en un sentido

estricto, en el que se señala que es cualquier acto ilícito penal, en el que las computadoras, sus técnicas y funciones desempeñan un papel (ya sea como método, medio o fin) (Ross & Sigüenza, 2010, p. 9).

Por su parte, Suárez-Sánchez (2009) resalta que, en conclusión, el delito informático está vinculado, no solo a la ejecución de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información *per se*, como bien jurídico tutelado, diferente de los intereses jurídicos tradicionales (Ojeda-Pérez et al., 2010, p. 49).

A raíz de los diferentes conceptos, por delitos informáticos o delitos cibernéticos se ha concluido que comprenden todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet que generan una afectación; o aquellas acciones u omisiones culpables realizadas por un ser humano, mediante un uso tecnológico, que causen un perjuicio a las personas, sin que necesariamente el autor logre un beneficio propio o a terceros (Soto, 1996, pp. 407- 410).

Los primeros orígenes de los delitos informáticos se pueden rastrear a partir de los años 60, inculcados por el temor de la literatura que poseía una relación con la recolección y el almacenamiento de datos personales en computadoras. De hecho, se toma como referencia la obra *1984*, de George Orwell, en la cual un gran hermano omnipresente controlaba y vigilaba la vida de las personas a través del uso de tecnologías (Corral Talciani, 2017, pp. 44-45). Tras la publicación de artículos periodísticos sobre algunos de los casos, aparecieron por primera vez los términos 'delitos informáticos' o 'delincuencia relacionada con computadoras', retomados posteriormente por la literatura fantástica de la época para la publicación de obras al respecto en un género que se denominó '*cyberpunk*' (Ávila et al., 2018, pp. 9-13).

> Los primeros estudios empíricos del delito informático se llevaron a cabo a mediados de los años 70, aplicando métodos científicos de investigación criminológica (División de Investigación y Desarrollo del Consejo Nacional de la Prevención del Delito, 1981). En un informe realizado por la División de Investigación, se identificó el primer caso de delito informático: 'el caso de John Draper', en septiembre de 1970 (también referido como 'el Captain Crunch'). Este descubrió que los obsequios ofrecidos en la caja de cereal Captain Crunch duplicaban perfectamente la frecuencia del tono 2600 Hertz de una línea de WATS y le permitían hacer llamadas telefónicas gratis. La gran víctima aquí fue la compañía AT&T. (Manjarrés Bolaño, 2012, p. 3)

Durante la década de los 70, se empezó a registrar una serie de casos que dejó pérdidas cuantiosas en el sector privado, delitos económicos como el espionaje informático, la piratería de *software*, el sabotaje y la extorsión (Zavydniak et al., 2022). En lo concerniente al espionaje, esto se llevaba a cabo mediante la copia directa desde los dispositivos informáticos (el robo directo de los mismos permitía la extracción de información de discos duros y *diskettes*) y la absorción de emisiones electromagnéticas para la captación de datos (Barrios, 2012, pp. 5-6).

Actualidad y evolución de los delitos informáticos

El mundo de la tecnología ha permitido que la sociedad evolucione significativamente, ya que, con el pasar del tiempo, esta ha sido fuente principal de comunicación. Ahora, resulta más práctico tener un dispositivo móvil o una computadora, dado que facilita la comunicación, la elaboración de trabajos por vía online, la creación de métodos de aprendizaje, entre otras utilidades. No obstante, no se debe dejar de lado el aumento del riesgo cibernético que enfrentan las personas que emplean el internet, puesto que son más susceptibles a sufrir daños y perjuicios (como el robo de identidad, la manipulación, el fraude, etc.).

En la actualidad, la tecnología se utiliza no solo como herramienta auxiliar de apoyo a diferentes actividades humanas (Pupo, 1990, p. 15), sino como medio eficaz para obtener y conseguir información, lo que también la habilita como un nuevo medio de comunicación que tiene como propósito mejorar el bienestar de los individuos. Según el diccionario de la Real Academia Española, el término 'informática' se define como el "conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales", los cuales están presentes en casi todos los campos de la vida moderna. Con mayor o menor rapidez, todas las ramas del saber humano se rinden ante los progresos tecnológicos y comienzan a utilizar los sistemas de información para ejecutar tareas que solían realizarse manualmente (Del Pino & Martín, 2007).

La información sobre la vida personal se está volviendo un bien muy cotizado por las compañías del mercado actual. La explosión de las industrias computacionales y de comunicaciones ha permitido la creación de un sistema que puede guardar grandes cantidades de información de una persona y transmitirla en muy poco tiempo. Cada vez más personas tienen acceso a esta información, sin que las legislaciones sean capaces de regularla.

La evolución de las computadoras, el aumento de la capacidad de almacenamiento y el procesamiento en estos dispositivos genera mayor amplificación

a la hora de guardar información, con lo cual se les facilita a los delincuentes el acceso a ella. La miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación y la investigación en el campo de la inteligencia artificial sirven como ejemplo del desarrollo actual (referido a menudo como la 'era de la información'). Con mayor propiedad, se podría decir que se está frente a la 'era de la informática' (Pons, 2017, p. 5).

Causas principales de los delitos informáticos

Según investigaciones, los delitos informáticos han incrementado con el pasar del tiempo. Se desconocía cuáles eran las razones para que estos aumentaran cada vez más, pero se sabe que la mayoría de los procesos guardaba relación con el uso ilegal de redes y de bases de datos. El área de justicia y seguridad proporciona asistencia técnica al Gobierno de Colombia, especialmente a la policía judicial y a los operadores de justicia, en cuanto a las técnicas específicas aplicadas a la evidencia digital y la planificación de acciones contra los delitos informáticos (robo de identidad, fraude financiero, *phishing*, *hacking*, sabotaje electrónico, crímenes contra menores y explotación sexual a través de medios electrónicos); así mismo, se trata de la vigilancia y el control que se ejecuta al momento de ingresar y navegar en internet, eso mismo sucede con las redes sociales, que, según Worldometers, son frecuentadas aproximadamente por 7800 millones de personas (Gonzáles et al., 2018, pp. 187-188).

Mundialmente, se dieron a conocer más de cien causas por las cuales el delito informático ha aumentado y aproximadamente cincuenta de ellas afectan a Colombia, como el *hackeo* de correos electrónicos de ministerios y de funcionarios de alto perfil, ya que se ha logrado encontrar información valiosa que deja en vulnerabilidad la integridad de cada uno de ellos (Miranda & Manzur, 1996). Por otro lado, debido a la facilidad con la que el autor del crimen puede permanecer inadvertido o anónimo, es mucho más sencillo cometer un crimen informático y salirse con la suya en el mundo cibernético que en el mundo real; sin embargo, la capacidad de rastrear direcciones de red IP está mejorando constantemente, lo que hace que sea más difícil mantenerse invisible en el internet (Fernández, 2014, p. 6).

Las redes de computación se extienden por todo el mundo, lo cual hace que sea muy difícil para cualquier Gobierno o departamento de seguridad de Estado

promulgar o hacer respetar el cumplimiento de las leyes cuando los perpetradores se encuentran en países extranjeros. En muchos casos, estos criminales reciben el apoyo de los Gobiernos locales en el intento de llevar a cabo el espionaje de computación o el ciberterrorismo y son capaces de cometer los crímenes por obligación a sus respectivos países sin temor a ser arrestados o detenidos (Medero, 2015, p. 75).

Algunos códigos de computación son maliciosos (como los virus) y suelen ser causados por alguien que intenta provocarle un daño a un individuo o una compañía, probablemente por haber perdido el empleo, presenciado una conducta inmoral de negocios o por celos o envidia; otra causa de los delitos informáticos es intentar destruir o dejar a sus objetivos imposibilitados para obtener la satisfacción personal de ver cómo sufren los efectos (Pizarro et al., 2016, p. 15).

Actualmente, se han visto casos de jóvenes que envían información muy íntima, a través del chat, y no necesariamente a personas conocidas. Las redes sociales proveen la facilidad de hablar y conocer a gente; hay quienes tienen suerte y dan con perfiles reales, pero hay quienes sufren el caso contrario. En consecuencia, exhibir la vida personal es algo de sumo cuidado. Existen plataformas (como Instagram) en las cuales se crean perfiles de 'tiendas virtuales' falsas que se encargan de extorsionar a las personas con productos que no existen, robando sus cuentas, adquiriendo información del lugar en dónde viven, su nombre, identificación y otros datos que dejan la dejan en gran estado de vulnerabilidad. Este es uno de los mecanismos más funcionales que utilizan los criminales para conseguir víctimas (Morduchowicz, 2012, p. 5).

Tipos, características o formas de cometer un delito informático

Se debe tener en cuenta la clasificación del delito informático para poder ampliar el conocimiento acerca de esta problemática. Para Téllez Valdés (citado en López, 2014), abogado e investigador de la Universidad Nacional, las principales características de los delitos informáticos son las siguientes:

a) **Son conductas criminales de cuello blanco.** Solo personas que tienen cierto tipo de conocimientos relacionados con la materia pueden ejecutarlos.
b) **Son acciones ocupacionales.** Ya que muchas veces, por su ubicación laboral, se maneja información de carácter netamente confidencial.

c) **Provocan serias pérdidas económicas.** Quien los ejecuta casi siempre lo hace para beneficiarse económicamente.
d) **Ofrecen posibilidades de tiempo y espacio.** Se pueden ejecutar en unos pocos segundos y sin importar en qué lugar se encuentre la persona (es decir que no se requiere estar presencialmente).
e) **Son muy sofisticados y presentan grandes dificultades para su comprobación.** Se requiere tener conocimientos muy amplios en esta materia (López, 2014, pp. 6-7).

Con el paso del tiempo y su evolución, se han conocido diferentes tipos de delitos informáticos (Serrano, 2014, pp. 15-16):

- **Estafa.** Es una de las actividades delictivas más antiguas. Las plataformas de interacción de información (redes sociales), junto con la era digital actual, han permitido que los estafadores realicen con éxito su plan desde cualquier lugar. Sin embargo, su propagación es desbordante, ya que las personas víctimas de esta transgresión no denuncian; algunas veces, por distintas circunstancias (como miedo e intimidación). Esta se ha convertido en la forma más usual en el mundo (Bacigalupo, 2007, p. 24).
- ***Skimming.*** Consiste copiar la banda magnética de una tarjeta (crédito o débito). Este acto delincuencial hace referencia al robo de información de tarjetas de crédito o débito en el momento de la transacción. Su finalidad es clonar las tarjetas de crédito o débito para proceder con la reproducción ilegal de información personal. Los ambientes más propicios en los que se da el *skimming* de una manera exitosa son los cajeros electrónicos, bares, gasolineras y restaurantes, dado que este método se puede ejecutar instalando un dispositivo que logre copiar la información de la tarjeta (Cano et al., 2014, pp. 12-13).
- **Carta nigeriana.** Es un tipo de estafa que consiste en ilusionar a la víctima con una fortuna inexistente y persuadirla para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna. Esta actividad ilegal también se conoce como 'estafa nigeriana'; hurto que tradicionalmente se realiza por medio de correos electrónicos que no suelen ser solicitados por parte de la víctima (algo así como el 'spam'). Paradójicamente, las personas que están detrás de este modelo de fraude revisten su acción pérfida de una intención lucrativa cuantiosa, por lo que este robo virtual siempre procura solicitar sumas bastante elevadas (Fernández, 2007, p. 22).

- ***Smishing.*** Es uno de los delitos más comunes, el más nuevo. Este crimen cibernético sustenta su ejecución a través de técnicas de ingeniería social por medio de SMS (mensajes de texto), dirigidos a las víctimas (usuarios). Los mensajes de texto hacen parte de las plataformas más propicias para la solicitud de datos. Si la acción negativa no funciona bajo este procedimiento, se procede a gestionar llamadas por parte del usuario y, por último, que la víctima ingrese a alguna página web infiltrada (Guerrero, 2020, p. 53).

Hay otras formas u modalidades comunes de cometer delitos informáticos:

- Estafa por suplantación de *SIM card*. Modalidad en la que el ciberdelincuente, aprovechando que el titular de una línea telefónica se encuentra de viaje o no puede atender llamadas, se presenta en las oficinas de empresas de operadores de telefonía móvil para obtener una *SIM card* nueva suplantando al titular. Luego, sincroniza las redes sociales y los productos financieros vinculados al número telefónico del titular, a fin de validar accesos que le permitan generar transferencias no consentidas. Durante el año 2017, en Colombia, se identificaron más de 1500 incidentes mediante esta nueva modalidad delictiva, los cuales generaron pérdidas por $7.690.000.000 millones de pesos (Valoyes, 2019, p. 5).
- Ciberadicción al daño físico y mental a menores de edad. Si un niño no cuenta con las habilidades necesarias para distinguir qué información es cierta y qué información es falsa, o para interactuar de forma segura en internet, es muy fácil que pueda verse comprometido en uno de estos grupos que promocionan un modelamiento de interacción a base de retos con fines de autolesión, cuya acción criminal atenta en contra de la vida y de su integridad. Un ejemplo de este tipo de cibercrimen fue conocido como 'la ballena azul' o 'el reto del hada de fuego', que provocaron suicidios y lesiones físicas y mentales de adolescentes y jóvenes. En Colombia, en el año 2017, se vieron afectados 6.498.746 usuarios jóvenes.
- Delitos contra el honor. La relación entre las transmisiones electrónicas y los delitos contra el honor se produce por la posibilidad de utilizarlas para calumniar o injuriar a alguien, sea de manera directa y personal, por medio de un e-mail dirigido al sujeto pasivo, lanzando el ataque contra el honor por medio del internet; de forma que las imputaciones hechas puedan ser conocidas por cualquier usuario de la red, mediante la lectura de un mensaje, una noticia, un comentario o un editorial en un periódico o en una revista editada en la red.

Derecho comparado: normatividad del derecho penal colombiano frente a Chile

Los delitos informáticos en Colombia están tipificados bajo una regulación penal; es decir, son juzgados por la rama del derecho penal también denominado las leyes penales. Son las normas promulgadas por el órgano legislativo que establecen los delitos y las penas.

En Colombia, los siguientes delitos están tipificados (Callegari, 2016, pp. 7-8):

- **Datos engañosos.** Alteración de datos al momento de ingresar al computador. Los datos se ingresan con omisiones o agregaciones que alteran su sentido y contenido.
- **Técnica salami.** Delito que puede cometerse en las empresas o instituciones donde hay movimiento de dinero. Consiste en sustraer pequeñas cantidades de activos de numerosas procedencias redondeando las cuentas.
- **Caballo de Troya.** En la codificación de un programa, se introducen un grupo de oraciones con el propósito de realizar funciones no autorizadas (se podría afirmar que este es el método de sabotaje más común).
- **Bombas lógicas.** Programas que se ejecutan en momentos específicos, rutinas *a posteriori*, según ciertas condiciones de tiempo y fecha.
- **Puertas con trampas y ataques asincrónicos.** El primero de ellos consiste en utilizar las interrupciones en la lógica de un programa y el segundo en aprovechar el funcionamiento asincrónico de un sistema operativo (en ambos casos, con fines delictivos).
- **Recogida de residuos.** Consiste en recoger los borradores, o sea la información residual impresa en papel o la que queda en la memoria. Esta recolección es una buena fuente para establecer la situación de una empresa y así poder cometer algún fraude.
- **Suplantación.** Logro de acceso por medios electrónicos o mecánicos a áreas controladas, a fin de sustituir a una persona o cosa.
- Con la promulgación de un marco jurídico que buscó prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, con fundamento en el artículo 44 de la Constitución Política de Colombia se estableció uno de los hechos más importantes para el mundo jurídico, por medio de la Ley 679 de 2001, que introdujo una nueva modalidad de

> delito cometido en el ciberespacio, con la tipificación de los actos sexuales con personas menores de catorce años, delitos por medios virtuales, que se consuman utilizando redes globales de información. Esta disposición ha sido derogada por la Ley 1236 de 2008, la cual, sin importar el medio a través de cual se cometa el delito, castiga los actos sexuales con menores de catorce años, aplicando penas privativas de la libertad que van de nueve a trece años (Salazar, 2011, p. 6).

La legislación colombiana hizo una adición al catálogo delictual. En la Ley 1273 de 2009, expedida en Colombia, que versa al respecto de los delitos informáticos, se hace una revisión de los delitos que atentan contra las principales características de calidad de la información (que, en últimas, son condiciones de seguridad confidencialidad, integridad y disponibilidad); lo que legalmente puede esperar el cliente de las organizaciones en las cuales ha depositado su confianza. Además, se estudiaron las bases jurídicas para el tratamiento de los delitos informáticos en Colombia, como la Ley 599 del 24 de julio de 2000 y la Ley 1273 del 5 de enero de 2009 (Hernández, 2009, pp. 10-11).

Como se mencionó, en el año 2009, se emanó una sanción legislativa proferida de la Ley 1273, la cual modifica el Código Penal y crea un nuevo bien jurídico tutelado, denominado 'de la protección de la información y de los datos'. Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones (Temperini, 2013, p. 11).

Ahora bien, en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio sobre la posibilidad de aplicar las leyes penales y armonizarlas en el plano internacional, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter transnacional, cuyo problema principal es la falta de una legislación unificada, lo cual facilita la comisión de los delitos. En 1986, la OCDE publicó un informe titulado "Delitos de informática: análisis de la normativa jurídica", en el que reseñó las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y recomendó una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (Del Pino & Martín, 2007, p. 38).

Por otro lado, en Chile, en junio de 1993, entró en vigencia la Ley 19.223, sobre delitos informáticos, con la finalidad de proteger un nuevo bien jurídico ("la calidad, pureza e idoneidad de la información, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se

obtengan"). Así mismo, se buscaba proteger el patrimonio, en el caso de los fraudes informáticos; la privacidad, intimidad y confidencialidad de los datos, como el espionaje informático; la seguridad y fiabilidad del tráfico jurídico y probatorio en el caso de las falsificaciones de datos probatorios vía medios informáticos; y el derecho de propiedad sobre la información (Del Pino & Martín, 2007, p. 38).

Esa es una Ley especial, extra Código y consta de 4 artículos:

- **Artículo 1.** El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.
- **Artículo 2.** El que, con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
- **Artículo 3.** El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
- **Artículo 4.** El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Adicionalmente, la Ley 19.223 contempla los delitos informáticos de sabotaje y espionaje informáticos (aunque no lo hace de una forma clara). Así pues, en el artículo 1, el inciso primero, alude a los daños que se puedan cometer contra el *hardware* (sea destruyéndolo o inutilizándolo); por lo tanto, no se trataría de un delito informático, sino de un delito de daños convencional. Sin embargo, el artículo 3 se registra la figura del sabotaje informático y se señala que se sancionará a quien maliciosamente altere, dañe o destruya los datos contenidos en un sistema). Por su parte, el espionaje informático quedó tipificado en los artículos 2 y 4.

A pesar de lo anterior, la Ley 19.223 no considera aquellas figuras como el *hacking* o el fraude informático. En cuanto a la penalidad (según el artículo 1, por ejemplo, en el caso de que alguien destruya dolosamente un computador), establece que puede recibir como castigo la pena de presidio menor en su grado medio a máximo, es decir, puede tener desde 541 días hasta 5 años de cárcel. En virtud del artículo 2, si ingresa indebidamente a un sistema para conocer información sin autorización, puede recibir desde 61 días hasta 3 años de

presidio. De acuerdo con el artículo 3, si alguien graba intencionalmente un virus en un sistema, puede ser castigado desde 541 días hasta 3 años de presidio. Finalmente, en virtud del artículo 4, un operador que dé a conocer dolosamente el contenido de la información guardada en el sistema informático puede recibir también presidio desde 541 días hasta 3 años y, si la persona es el responsable del sistema, la pena puede alcanzar los 5 años (Cavada, 2020, p. 22).

En conclusión, con respecto de esta normatividad, se puede decir que las falencias en las que incurre en lo relacionado con la regulación de la delincuencia informática son evidentes; no obstante, hay que reconocer que esta es la pionera en la región en abordar expresamente el tema de los delitos informáticos. Por ejemplo, el fraude informático, entendido como la modificación incorrecta del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos (que se introducen o que ya están contenidos en el computador) en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de un tercero (Berríos, 2011, pp. 15-16).

En la normatividad chilena, a diferencia de la colombiana, se mencionan nuevas manipulaciones que llevan a las víctimas a ser el blanco de los delincuentes, y, así mismo, a cometer delitos informáticos. La 'manipulación de *input*' es una de las más frecuentes y consiste en el suministro de datos falsos al computador, sea modificando datos reales o introduciendo datos completamente ficticios. También se puede producir por la omisión de un registro de datos, lo cual deja a las víctimas desprotegidas y expuestas a quedar en manos del delincuente

Es menester identificar que Chile cuenta con instituciones especializadas como el Ministerio Público que investiga los actos que constituyen delitos y están establecidos en los artículos 80-A y 80-B de la Constitución chilena. El Ministerio Público es el único responsable de llevar a cabo las investigaciones de los hechos que constituyen delitos, incluido el delito cibernético y de ejercer el enjuiciamiento público penal, según lo dispuesto en su Ley Orgánica Constitucional (Cisternas & Moyano, 2007, p. 23).

La Policía de Investigaciones de Chile tiene una unidad de investigación especializada en ciberdelincuencia: la Brigada Metropolitana de Investigación de Delitos Cibernéticos. Fue activada en octubre de 2000 y sus funciones principales son detectar e investigar conductas ilegales en internet, proporcionar evidencia a los tribunales y fiscales y brindar capacitación y formación en investigación y en delitos informáticos. Está compuesta por tres áreas: Delitos en Internet contra los Niños, Delitos Informáticos e Informática Forense. Chile también cuenta con

un Centro de Respuesta a Incidentes de Computación y Seguridad (CSIRT-CL), que está patrocinado por el Ministerio del Interior y Seguridad Pública (Gamba, 2019, p. 98).

Según investigaciones, Alemania, Francia, Venezuela, Estados Unidos, Austria, entre otros, han sido los países con más desequilibrio financiero entre sus habitantes, debido a que han sido víctimas de espionaje de datos, estafa informática, falsificación de datos, falsedad ideológica, alteración de datos y sabotaje informático y tentativa o utilización abusiva de cheques o tarjetas de crédito. Lo anterior ha suscitado gran inconformidad y ha causado muchos daños a la sociedad (Candelario Samper & Bolaño, 2015, pp. 158-159).

Una vez analizada la legislación sobre el delito informático o ciberdelito, desde la perspectiva del derecho comparado, se puede concluir que existe diversidad de criterios, no unificados ni tipificados, que impiden establecer un estándar internacional; especialmente, cuando se trata de analizar la legislación existente en un país como Colombia, en comparación con otros Estados de la comunidad internacional (Rapp, 2001, p. 35).

Cada uno de los países tiene su respectivo marco jurídico dependiendo de la influencia histórica. Para el caso colombiano, existen diferencias frente a Chile; sin embargo, también existen similitudes en la modalidad en la que se cometen dichos delitos y en la vulneración que afecta a la población. Por otro lado, se llega a la conclusión que Colombia, en cuanto a las condenas que se imponen por los hechos cometidos que consuman los delios informáticos, tienden a ser un poco más rígidos con su normatividad.

Vulneración de los derechos fundamentales por causa de los delitos y la manipulación informática

Para entrar en contexto, es importante destacar que los derechos fundamentales se encuentran consagrados en la Constitución Política de Colombia y se definen como aquellos que son inherentes a cada persona; es decir que se nace con ellos y las leyes no deben ser contrarias a estos. Hay diversos, sin embargo, uno de los más importantes (y que abarca todos los aspectos) es el derecho a la vida, el cual es inviolable "artículo 3", la noción de derechos fundamentales nos remite a libertades, facultades de las personas que promueven su dignidad vital por su sola condición humana (Monteros, 2016, p. 15).

A partir de la Declaración Universal de los Derechos Humanos, adoptada por la Asamblea General de las Naciones Unidas, el 10 de diciembre de 1948, se dio identidad jurídica a la voluntad humana de respetarse y ser respetado por todos. Sobre todo, a partir de la incorporación de este cuerpo legal, entre otros instrumentos internacionales, en las constituciones de los Estados, tal como ocurrió en Argentina desde 1994. Este hecho no solo constituyó un acto legal y político importante, sino que ha generado obligaciones de las naciones hacia su propio interior, como en la relación internacional con otros Estados (González, 2016, p. 44).

Específicamente, el artículo 2 de la Constitución Política de Colombia establece que "toda persona tiene todos los derechos y libertades proclamados en esta Declaración, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición" (1991, p. 3). Mediante este y otros artículos se entiende que la población está sujeta y protegida por la legislación colombiana, pero eso no ha sido suficiente, ya que, como se ha tratado a lo largo de este capítulo, la problemática principal es la vulneración a los derechos fundamentales de las personas (Romero, 2015, p. 25).

La vulnerabilidad que caracteriza a las(os) niñas(os) y las(os) jóvenes en su relación con las nuevas tecnologías ha aumentado, por causa de la imposibilidad de tener certeza acerca de la identidad de las personas con quienes se conectan, sus intenciones y aspiraciones en estos vínculos virtuales establecidos. Se trata de relaciones cibernéticas, que se convierten en íntimas más rápidamente que en el mundo real, por la distancia emocional que impone el uso de una pantalla y que puede dar lugar a contactos físicos riesgosos cuando media el engaño (Burgos, 2010, p. 216). A partir de la publicación de fotos, una persona puede convertirse en víctima de sextorsión; es decir, sufrir chantajes bajo la amenaza de mostrar estos contenidos en espacios que las(los) niñas(os) o adolescentes necesitan preservar. La red facilita el actuar ilegal, dado que favorece el anonimato del actor y maximiza los efectos de la amenaza. Se trata de un medio que permite la actualización constante del material y el intercambio entre usuarios, sin límite ni fronteras (Flores, 2012, pp. 22-24).

El Estado colombiano ha planteado diferentes mecanismos e implementado estrategias a fin de prevenir y combatir los delitos informáticos. Por ejemplo, se ha modificado el control y el acceso a la información personal; se han regulado nuevos esquemas para que las personas ingresen con más seguridad; las redes sociales han restringido los contenidos obscenos que se pueden subir en los

perfiles de los usuarios y se ha implementado la opción de denunciar toda publicación que perturbe la tranquilidad; la entidad financiera o bancaria se encarga de asegurarse que la persona que realice una transacción sea efectivamente la titular de la cuenta, mediante vía telefónica y/o un mensaje de texto, con el fin de que se tenga información sobre el manejo de los productos y se evite que sea víctima de fraude (Esteban, 2001, p. 324).

Para finalizar, la Corte Constitucional, en su sentencia C-224/19, identifica los derechos a la vida e intimidad de las personas, así como el tratamiento de datos personales siendo una garantía y principio constitucional frente a los delitos que se consuman en el ciberespacio. Con el fin de respaldar los principios constitucionales y robustecer el marco normativo contra el cibercrimen, se realizó el Convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest. Se estipula que un convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio de Budapest, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable.

De acuerdo con lo contenido en esta sentencia, se tomaron ciertas medidas que deben cumplirse y adoptarse a nivel nacional:

- **Reforma o adecuación de conductas ilícitas.** Una de las medidas adoptadas a nivel nacional es en el derecho penal sustantivo, que es el conjunto de normas o leyes relativas a los delitos, a las penas y a las medidas de seguridad y con las cuales cuenta el Estado para eliminar la presencia de conductas antisociales, es decir, como lo estipula la sentencia, serían los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, siendo de gran ayuda para el cumplimiento y garantía en la sociedad.
- **Interferencia en los datos.** Cada parte adopta las medidas legislativas que resulten necesarias para tipificar como delito, en su derecho interno, la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.
- **Interferencia en el sistema.** Se busca la protección de la información y se establece que quien cometa un acto contrario a lo estipulado debe

tener su sanción respectiva y que no se debe dejar pasar por alto los daños ocasionados que provoquen una obstaculización grave y actuación ilegítima.

Así mismo, la Corte Constitucional estableció en la sentencia que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: dispositivos, contraseñas y datos informáticos, como abuso de los dispositivos, debe ser una conducta típica, antijurídica y culpable, dado que, por este medio se ejecuta una alta cifra de vulneración a la población. También los delitos relacionados con la pornografía infantil, entendiéndose como todo material pornográfico que contenga la representación visual de: 1. un menor comportándose de una forma sexualmente explícita, 2. una persona que parezca un menor comportándose de una forma sexualmente explícita y 3. imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

Conclusiones

Los delitos informáticos, como delitos transnacionales, presentan un grave problema que abarca diversos ámbitos nacionales y supranacionales; por consiguiente, su adecuación normativa es de suma importancia, dado que constituye una herramienta de salvaguarda ante una eventual violación a los derechos que le asisten a los individuos (desde el acceso a su información personal hasta la confidencialidad que se deriva de este). En efecto, para el Estado colombiano, este uso indebido constituye un delito que no se limita a las actuaciones que tienen lugar en el territorio. En definitiva, el traspaso de información, sin consentimiento, trasciende las fronteras y dificulta el manejo en lo que respecta a la justicia y su aplicación extraterritorial.

Aunado a ello, la información que se adquiere por medio de dispositivos electrónicos, así como la que reposa en las bases de datos de las organizaciones, es comercializada de manera indiscriminada, e incluso suele tener mayor oferta y demanda aquella que pertenece o está relacionada con los menores de edad. Lo anterior permite la configuración de otras conductas, como la pornografía infantil, que van en contravía absoluta del interés superior de los menores y la protección incondicional de los derechos que les son inherentes y que reposan en los instrumentos de los sistemas nacionales, regionales y universales de protección a los Derechos Humanos.

Referencias

Ávila Umaña, J. A., Barrera Argueta, A. A., & Monjaraz Díaz, F. J. (2018). *Elementos diferenciadores del delito de estafa regulado en el artículo 215 del código penal con la estafa informática regulada en la Ley Especial contra Delito Informático y Conexos*. Universidad de El Salvador. https://tinyurl.com/kf32yrxj

Bacigalupo, E. (2007). *Falsedad documental, estafa y administración desleal*. Marcial Pons. https://tinyurl.com/35kc3puh

Barrios Solano, S. A. (2012). *El delito informático en la legislación colombiana* [Tesis doctoral]. https://tinyurl.com/39m6y6f9

Burgos, Á. (2010). El delito informático. *Acta Académica*, (47), 175-199. https://tinyurl.com/4abbtwm9

Callegari, N. (2016). Delitos informáticos y legislación. *Revista de la Facultad de Derecho y Ciencias Políticas*, (70), 111-118.

Candelario Samper, J. J., & Bolaño, M. R. (2015). Seguridad informática en el siglo XX: una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales. *Publicaciones e Investigación, 9*, 153-162. https://tinyurl.com/ymu8sya3

Cano Cuervo, A., Díaz Heredia, J. M., Mendieta Vargas, C. C., Rivas Sánchez, C. C., & Sánchez Carvajal, N. F. (2014). *Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes* [Tesis Bachelor's, Universidad Libre]. https://tinyurl.com/2p97wyd2

Cavada, J. (2020). *Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera*. Asesoría Técnica Parlamentaria, Biblioteca del Congreso Nacional de Chile. https://tinyurl.com/5ctydz8e

Cisternas Hernández, E. A.. & Moyano Montecino, J. (2007). *Análisis y proyección de los delitos informáticos en Chile* [Tesis doctoral, Universidad de Talca (Chile)]. http://dspace.utalca.cl/handle/1950/4932

Corral Talciani, H. F. (2017). El derecho al olvido en internet: antecedentes y bases para su configuración jurídica. *Revista Jurídica Digital UANDES, 1*(1), 43-66. https://tinyurl.com/yck43yan

Del Pino, S., & Martín, S. (2007). *Delitos Informáticos: Generalidades*. Fiscalía General del Estado, Ecuador. https://tinyurl.com/z6rn3jas

Esteban, M. (2001). Internet y los derechos fundamentales. *Anuario Jurídico de La Rioja*, (6-7), 321-356. https://tinyurl.com/4kfsbbrs

Fernández, H. (2014). *Manual de Derecho informático*. Abeledo Perrot. https://d1wqtxts1xzle7.cloudfront.net

Fernández, J. (2007). Respuesta penal frente a fraudes cometidos en Internet: estafa, estafa informática y los nudos de la red. *Revista de Derecho Penal*, (19). https://tinyurl.com/bddp68ce

Flores, J. (2012). Cómo se origina la sextorsión. *Sextorsión*. https://tinyurl.com/bdez7bbk

Gamba, J. (2019). *El delito informático en el marco jurídico colombiano y el derecho comparado: caso de la transferencia no consentida de activos* [Tesis de maestría]. Universidad Externado de Colombia. https://tinyurl.com/4ffe9d2k

Gonzáles, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). Delitos informáticos: una revisión en Latinoamérica. *Conference Proceedings, 2*(2), 178-190. https://tinyurl.com/2p83v3jt

González, Y. (2016). *Análisis de los delitos informáticos fijados por la ley 1273 de 2009 en relación con las redes sociales en Colombia* [Tesis de grado]. Universidad Católica de Colombia. https://tinyurl.com/yysf4n22

Guerrero, J. (2020). *Incidentes informáticos en Colombia en los últimos 10 años* [Monografía de grado]. Universidad Nacional Abierta y a Distancia. https://tinyurl.com/2p83ack5

Gutiérrez, M. (1991). *Fraude informático y estafa: aptitud del tipo de estafa en el derecho español ante las defraudaciones por medios informáticos*. Ministerio de Justicia.

Hernández, L. (2009). El delito informático. *Eguzkilore*, (23), 227-243. https://tinyurl.com/yckb3zyd

Lima, M. (1984). *Delitos electrónicos*. Editorial Porrúa.

López, J. (2014). *Criminalidad informática en Colombia*. Universidad La Gran Colombia. https://tinyurl.com/2s3e7jt2

Manjarrés Bolaño, I. (2012). Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano, 5*(9). https://tinyurl.com/yrp2n9r2

Medero, G. S. (2015). El ciberterrorismo: de la web 2.0 al internet profundo. *Revista de cultura y ciencias sociales, 85*, 100-108. https://tinyurl.com/4rxw6x3s

Miranda, M. H., & Manzur, C. L. (1996). *Delitos informáticos*. Editorial Jurídica ConoSur.

Monteros, J. I. (2016). *Los operadores de justicia frente a los delitos informáticos* [Tesis de maestría]. https://tinyurl.com/227mbsda

Morduchowicz, R. (2012). *Los adolescentes y las redes sociales*. FCE. https://tinyurl.com/bdhe9nkk

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de contabilidad, 11*(28). https://tinyurl.com/bdh4wadx

Pizarro Román, C. E., Díaz Bazán, R. A., & Vigo Florián, E. (2016). *Seguridad y prevención ciudadana*. Universidad Alas Peruanas. https://tinyurl.com/z9t289dn

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, (20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Pupo, R. P. (1990). *La actividad como categoría filosófica*. Editorial de Ciencias Sociales. https://tinyurl.com/y67a4s7k

Rapp Ortega, R. (2001). *El delito informático en Chile y en el derecho comparado* [Tesis de grado]. Universidad de Chile. https://tinyurl.com/2485tatw

Romero Roa, L. F. (2015). Seguridad informática en Colombia. *Re-Pilo*. https://tinyurl.com/mwmjjrap

Ross, P., & Sigüenza, S. (2010). *Factores de riesgo que predisponen a los adolescentes de una institución educativa privada, al uso adictivo de las redes sociales en internet* [Tesis inédita]. Universidad Rafael Landívar.

Salazar, J. F. (2011). Situación normativa de la Sociedad de la Información en Colombia. *Criterio Jurídico, 9*(1). https://tinyurl.com/5n6edbhv

Salvadori, I. (2010). La lucha contra el hurto de identidad. Las diferentes perspectivas legislativas. En *El robo de identidad. De la política criminal internacional a la práctica* (pp. 77-94). Navarra.

Serrano Buitrago, E. R. (2014). *La práctica de delitos informáticos en Colombia* [Trabajo de grado de especialización]. Universidad Militar Nueva Granada. https://tinyurl.com/2p89tcwv

Soto, C. F. (1996). Aspectos metodológicos del delito informático. *Informática y derecho: Revista iberoamericana de derecho informático*, (9), 407-412. https://tinyurl.com/2p8bdawb

Suárez-Sánchez, A. (2009). *La estafa informática*. Grupo Ibáñez.

Temperini, M. G. I. (2013). Delitos informáticos en Latinoamérica: un estudio de derecho comparado. *1ra. Parte. In 1er. Congreso Nacional de Ingeniería Informática/Sistemas de Información*. https://tinyurl.com/4hc8bmrv

Valoyes Mosquera, A. (2019). *Ciberseguridad en Colombia* [Trabajo de grado de especialización]. Universidad Piloto de Colombia. https://tinyurl.com/3nan8czb

Zavydniak, V.I., Zavydniak, I.O., Omelchuk, L.V., Polunina, L.V. & Suprun-Kovalchuk, T.M. (2022). States' main directions and forms of in-ternational cooperation in the fight against transnational economic crimes. *Revista Científica General José María Córdova, 20*(38), 323-339. https://dx.doi.org/10.21830/19006586.904