Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera

Autor

Juan Pablo Cavada Herrera
Email: jcavada@bcn.cl
Tel.: (56) 32 226 3905

Nº SUP: 126200

Resumen

El término "cibercrimen" carecería de una definición universalmente homogénea y aceptada por los especialistas en el área, existiendo eso si acuerdo entre los investigadores en que sería una actividad ilegal realizada mediante un computador.

De las distintas definiciones doctrinales y de instrumentos internacionales, se desprenden diferentes conceptos, tales como delincuencia informática, abuso informático, criminalidad informática, criminalidad mediante computadoras, delitos informáticos, etc. Estos, se refieren, más que a una forma específica de delito, a una pluralidad de modalidades delictivas, vinculadas de algún modo con los computadores, designando una multiplicidad de conductas ilícitas y no una sola de carácter general, y parece hablarse de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.

En síntesis, "delito cibernético" sería una acepción amplia, que comprende situaciones en que el elemento informático se encuentra en el objeto de la conducta penada (por ejemplo, intromisión ilegal a bancos de datos), y aquellas en que dicho elemento es el medio para realizar un fin ilícito.

De esta manera, el concepto de cibercrimen abarcaría, en sentido amplio, tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. Y dentro de este término genérico, los delitos informáticos serían aquellas conductas delictuales en que se atacan bienes informáticos en sí mismos, no como medio, como por ejemplo, dañar el *Software* mediante la intromisión de un virus.

Introducción

El presente informe intenta dilucidar, a partir de diferentes autores, la diferencia entre los conceptos "cibercrimen" y "delito informático". La revisión efectuada no agota la posibilidad que otros autores se pronuncien sobre lo mismo. Luego, se analiza si la legislación internacional y/o algunas legislaciones extranjeras regulan ambas materias por separado, suponiendo que realmente sean materias distintas.

Las traducciones son propias.

I. Algunas definiciones doctrinales

Rodríguez Flores (2013) señala que el término “cibercrimen” carecería de una definición universalmente homogénea y aceptada por los especialistas en el área, existiendo acuerdo entre los investigadores en que sería una actividad ilegal realizada mediante el computador. Sin embargo, continúa el autor, habría desacuerdo sobre el lugar en que se ejecuta tal actividad, y tales diferencias se evidenciarían en las definiciones del señalado delito:

- Chung (2004) lo define como actividades ilegales realizadas a través de computadores que a menudo tienen lugar en las redes electrónicas globales.
- Parker (1998) afirma que es el sistema de información que sirve de canal.
- Philippsohn (2001) considera que se realizan a través de internet.
- Power (2002) lo define como la intromisión sin autorización de un computador.
- Chawki (2005) indica que el computador tiene varios roles en el cibercrimen, pues sirve de objeto, sujeto, herramienta y símbolo. A su vez, sostiene que se diferencia en cuatro formas de los llamados crímenes territoriales: permiten un fácil aprendizaje de cómo realizarlos, requieren pocos recursos en comparación con el daño potencial que pueden ocasionar, pueden ser cometidos en una jurisdicción sin necesidad de estar físicamente presente y frecuentemente no son claramente identificados como ilegales.

Por su parte, Kleve, De Mulder y van Noortwijk (2011), citados por Rodríguez Flores (2013), señalan la importancia de investigar el cibercrimen, por la necesidad de conocer cómo opera, para diseñar las investigaciones criminales, por la percepción de que las leyes convencionales no se aplican a este tipo delitos, ya sea por no estar explícitas o por la forma en que se interpreten, y por la insuficiencia de un manejo seguro de la infraestructura que ofrece internet. Enfatizan en que este tipo de delitos dependen del conocimiento, en lo que sucede dentro de un sistema automatizado y cómo se estructura, beneficiándose además de un vacío en la legislación, dada la posibilidad de que la autoridad del Estado pueda estar indeterminada en dicho espacio.

Luego, Salom, Chawki, Speer (Tips, 2013), refiriéndose a los desafíos de la regulación del cibercrimen, y a los sujetos amenazados por éste, mencionan distintos tópicos, utilizando el término “delito informático”, pero refiriéndose principalmente a la ciberseguridad en el manejo de datos (Rodríguez Flores, 2013).

También hay quienes hacen sinónimo ambos términos, al señalar que se entiende por “ciberdelito” o “cibercrimen” cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito (Rayón y Gómez, 2014: 209-234).

En el mismo sentido, homologando se dice que delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet (13° Congreso sobre Prevención del Delito y Justicia Penal, 2005).

De la misma manera hay quien señala genéricamente que la diferencia entre el delito informático y el ciberdelito es que el primero se vale de elementos informáticos para su perpetración, mientras que el segundo se refiere a una posterior generación delictiva vinculada a las tecnología de la información y comunicaciones (TIC) en el que interviene la comunicación telemática abierta, cerrada o de uso restringido (Romeo Casabona, 2006:1-42).

En este sentido, se dice que la criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, son llevados a cabo utilizando un elemento informático (Cuervo, 2008).

Rayón y Gómez (2014) sintetizan a diversos autores, señalando que los ciberataques son una categoría de ilícito más amplia que los delitos informáticos, pues los ciberataques incluirían conductas criminales que no constituirían delitos, pero que si formarían parte de la criminalidad informática.

Y así, de las distintas definiciones recopiladas por Rayón y Gómez (2014), se puede ver que numerosos autores e instituciones (Gómez Perals, Ruiz Vadillo, recomendaciones de la OCDE, Consejo de Europa, Ruiz Vadillo, Comité de Ministros del Consejo de Europa, Baón Ramírez, Tiedemann, Sarzana, Callegari, Rodríguez, Téllez Valdés, entre otros), se refieren y definen distintos conceptos, tales como delincuencia informática, abuso informático, criminalidad informática, criminalidad mediante computadoras, delitos informáticos, etc., bajo determinados enfoques doctrinales, refiriéndose, más que a una forma específica de delito, a una pluralidad de modalidades delictivas vinculadas, de algún modo con los computadores, designando una multiplicidad de conductas ilícitas y no una sola de carácter general, y parece hablarse de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular (Rayón y Gómez, 2014).

II. Instrumentos internacionales y su recepción nacional, en particular en Chile

1. Convenio de Budapest sobre la Ciberdelincuencia

De acuerdo a Naciones Unidas, los llamados delitos informáticos, o delitos cibernéticos, en sentido estricto, son aquellos que implican un “comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos o los datos procesados por ellos” (BCN, 2014).

El 23 de noviembre de 2001, la Unión Europea junto a Estados Unidos de América, Canadá, Japón y Sudáfrica, firmaron el Convenio de Budapest sobre la Ciberdelincuencia (en adelante, el Convenio), cuyo objetivo es intensificar la cooperación entre los Estados firmantes en la lucha contra la

cibercriminalidad y en la protección de los intereses vinculados a las TIC's, a favor de ofrecer respuestas eficaces, rápidas y coordinadas en la detección, investigación y persecución de estos delitos. Para ello, se comprometieron a adoptar medidas necesarias para prever como infracción penal a todas aquellas acciones que atentan contra la propiedad intelectual, la intimidad, el contenido, el acceso no autorizado y el sabotaje. Adicionalmente, definieron el derecho procesal, las condiciones y garantías, así como los lineamientos de cooperación internacional que regirán su acción.

Salom, citado por Rodríguez Flores (2013), indica que en este Convenio se agruparon los delitos informáticos en cuatro grupos:

- Delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas informáticos (acceso e interpretación ilícita así como la interferencia de datos).
- Delitos por su contenido, tales como la pornografía infantil y xenofobia.
- Delitos relacionados con la informática, como la falsificación y fraude.
- Delitos relacionados con las infracciones a los derechos de propiedad.

2. Legislaciones latinoamericanas y el Convenio de Budapest sobre la Ciberdelincuencia

Las respuestas ofrecidas por los países de la región, que firmaron el Convenio, consistirían principalmente en modificar la legislación penal (Argentina, Bolivia, Costa Rica, Guatemala, México, Paraguay y Perú), seguido por la introducción de leyes específicas (Brasil, Chile, Colombia y Venezuela)[1].

Ecuador, por su parte, ha usado una ley civil y comercial para introducir sanciones penales, mientras que Uruguay solo prevé una ley de protección a los derechos de autor.

En los países en que no ha habido aún una reforma en este campo, se trata de "reinterpretar" la normativa vigente en materia penal para incluir la tipología de delitos informáticos (Rodríguez Flores, 2013).

3. Chile y el Convenio de Budapest

Si bien el Convenio no define ciberdelincuencia ni delitos informáticos, en Chile, el Decreto N° 83, de 2017, del Ministerio de Relaciones Exteriores, que promulga el Convenio de Budapest, puede dar

[1] El Artículo 37° del Convenio permite la incorporación a éste, de países que no sean miembros del Consejo de Europa. A julio de 2018 el Convenio había sido ratificado por 60 Estados. Junto a los Estados miembros de la Unión Europea, el Convenio ha sido ratificado por países no europeos , entre ellos Estados Unidos, Canadá, Australia, Japón, Israel, República Dominicana, Chile, Argentina, Colombia. Otras organizaciones internacionales han adherido a él, tales como la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de los Estados Americanos (OEA), la Oficina de Naciones Unidas contra la Droga y el Delito (UNODC), y la Unión Internacional de Telecomunicaciones (UIT) (COE, *Chart of signatures and ratifications of Treaty* 185). (BCN, 2018).

indicios de que se entiende por ciberdelincuencia, gracias a las normas contenidas en la Declaraciones al Convenio y en las Reservas al mismo.

En cuanto a las Declaraciones al Convenio sobre la Ciberdelincuencia, el Decreto dispone:

a) La República de Chile declara que exigirá una intención delictiva determinada en el sujeto activo para penar las acciones descritas en los artículos 2 y 3 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el artículo 2 de la Ley N° 19.223 sobre delitos informáticos.

b) La República de Chile declara que exigirá un ánimo fraudulento que produzca un perjuicio a terceros para penar las acciones descritas en el artículo 7 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el artículo 197 del Código Penal.

A su vez, el artículo 2 del Convenio se refiere al "acceso ilícito", obligando a la tipificación como delito el acceso deliberado e ilegítimo a todo o parte de un sistema informático, pudiendo exigir los Estados, que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático. El artículo 3 se refiere a la "interceptación ilícita", obligando a los Estados partes, a tipificar como delito la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, pudiendo exigir los estados, que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Por su parte, el artículo 2 de la Ley N° 19.223 sobre delitos informáticos, recogiendo ambos conceptos (acceso e interceptación ilícita) para su penalización, dispone que,

> El que con el ánimo de apoderarse, usar o conocer indebidamente de 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.

Por otra parte, el artículo 7 del Convenio, al que se remite el decreto promulgatorio, obliga a los Estados a tipificar el "delito de falsificación informática", consistente en la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente, pudiendo exigir los Estados, que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Para efectuar esa tipificación, el Decreto promulgatorio declara que Chile exigirá un ánimo fraudulento que produzca un perjuicio a terceros, conforme lo requiere el artículo 197 del Código Penal, que a su vez se refiere a la falsificación de instrumento privado con perjuicio de terceros.

Por lo tanto, si bien el Convenio se refiere a la "ciberdelincuencia" y a los delitos informáticos, sin definirlas, sus artículos 2, 3 y 7 obligan a los Estados parte a tipificar en sus legislaciones delitos de acceso deliberado e ilegítimo a un sistema informático; la interceptación deliberada e ilegítima por medios técnicos de datos informáticos; y de falsificación informática, y en todos ellos, Chile se compromete a tipificarlos, pero exigiendo en ellos una intención delictiva determinada en el sujeto activo (artículos 2 y 3 del Convenio) y ánimo fraudulento que produzca un perjuicio a terceros (artículo 7 del Convenio).

En otros términos, el Convenio obliga a tipificar conductas en que el medio o elemento informático es un objeto de la conducta típica, y no solo un medio para cometer el delito. En ese sentido, Chile declara adoptar dichas directrices. Otro aspecto, que no es analizado en este informe, es si efectivamente la Ley N° 19.223 contempla delitos informáticos bajo esta premisa, o si, también incluye otras figuras en que el elemento informático no sea un objeto del delito, sino un simple medio de comisión, o si incluso siendo un objeto del delito, no requiere ser atacado por medios informáticos (por ejemplo, si un delito de daños cometido respecto de un computador por medios físicos es considerado un delito informático en Chile).

III. Estados Unidos de América

En cuanto al concepto de "delito cibernético", la legislación estadounidense es pionera en la materia, acuñando el concepto (*cybercrime*), utilizando una acepción amplia del mismo, que comprende aquellas situaciones en que el elemento informático se encuentra en el objeto de la conducta penada (por ejemplo, intromisión ilegal a bancos de datos), y aquellas en que dicho elemento es el medio para realizar un fin ilícito (por ejemplo, estafa por Internet) (BCN, 2014).

De esta manera, el concepto de cibercrimen (o ciberdelitos) en sentido amplio, abarca tanto delitos comunes que se ejecutan a través de medios informáticos, como nuevos delitos, cuya ejecución sólo es posible gracias a la existencia de dichos medios. Esto implica que la respuesta a este tipo de criminalidad apele tanto a la legislación general como a leyes especialmente diseñadas para combatirla, sin perjuicio de que se critique la inadecuación de la legislación basada en la jurisdicción estatal para perseguir un fenómeno de alcance global.

Luego, la legislación norteamericana tipifica bajo de denominación genérica de ciberdelitos figuras de terrorismo (Ley USA PATRIOT), obscenidades, diversas figuras de pornografía, prohibición de dominios engañosos, prohibición de uso de recursos públicos para adquisición de ordenadores sin filtros, seducción de menores para propósitos sexuales, protección de *copyright*, difamación, amenazas y acoso cibernético, etc., todos ellos cometidos por medios informáticos (BCN, 2014).

Fuentes normativas

Código Penal. Disponible en: http://bcn.cl/1uvs0 (julio, 2020).

Convenio sobre la Ciberdelincuencia, Budapest, 23 de noviembre de 2001. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf (julio, 2020).

Decreto N° 83, de 2017, Ministerio de Relaciones Exteriores, Promulga Convenio sobre la Ciberdelincuencia. Disponible en: https://www.leychile.cl/Navegar?idNorma=1106936 (julio, 2020).

Referencias

Biblioteca del Congreso Nacional, BCN (2014). Los delitos cibernéticos en la legislación estadounidense. Matías Meza-Lopehandía. Disponible en: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf (julio, 2020).

Biblioteca del Congreso Nacional, BCN (2019). Convenio sobre la Ciberdelincuencia: Convenio de Budapest. Disponible en: https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf (junio, 2020).

Cuervo, José (2014). Delitos informáticos: Protección penal de la intimidad. Disponible en: http://www.informatica-juridica.com/trabajos/delitos.asp (julio, 2020).

Naciones Unidas (2015). 13º Congreso sobre Prevención del Delito y Justicia Penal, Doha, 2015, 12 al 19 de abril. Disponible en: https://www.un.org/es/events/crimecongress2015/about.shtml (julio, 2020).

Rayón Ballesteros, y Gómez Hernández (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, XLVII (2014). Disponible en: https://dialnet.unirioja.es/descarga/articulo/4639646.pdf (julio, 2020).

Rodríguez Flores, María Eugenia (2013). América Latina, ¿Debe crear un sistema de normas armonizadas para el cibercrimen? Trabajos de Investigación en Políticas Públicas, N° 16, 2013. Departamento de Economía de la Universidad de Chile. Disponible en: http://www.econ.uchile.cl/uploads/publicacion/9ba7739a0ac26598402dab53c990c58e49fc259a.pdf (julio, 2020).

Romeo Casabona, Carlos (2006). “De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal” en El cibercrimen nuevos retos jurídico-penales, nuevas respuestas político-criminales. Editorial Comares. Granada.

Nota aclaratoria

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.