Biblioteca del Congreso Nacional de Chile

Convenio de Budapest sobre la ciberdelincuencia

Serie Minuta Nº 121-23, 06/11/2023

por Blanca Bórquez Polloni

Resumen

La presente Minuta tiene por objeto servir de insumo a los parlamentarios chilenos que participarán en los talleres nacionales sobre ciberdelincuencia organizados por el Foro de Presidentes de Poderes Legislativos (FOPREL) en colaboración con el Consejo de Europa, a través de su proyecto (GLACY+). Estos tendrán lugar en República Dominicana los días 7 y 8 de noviembre, y en México el día 10 del mismo mes.

El objetivo de estos talleres es fortalecer las legislaciones nacionales de ambos países, teniendo por base el Convenio de Budapest sobre ciberdelincuencia del Consejo de Europa y sus Protocolos, instrumento al cual hace referencia el presente documento.

Disclaimer: Este trabajo ha sido elaborado a solicitud de parlamentarios del Congreso Nacional, bajo sus orientaciones y particulares requerimientos. Por consiguiente, sus contenidos están delimitados por los plazos de entrega que se establezcan y por los parámetros de análisis acordados. No es un documento académico y se enmarca en criterios de neutralidad e imparcialidad política.

TABLA DE CONTENIDOS

1. Introducción

El Foro de Presidentes de Poderes Legislativos (FOPREL), con el objeto de fortalecer los marcos normativos de República Dominicana y México en materia de cibercrimen, se ha propuesto realizar talleres en colaboración con el Consejo de Europa, en los cuales se tenga por base el Convenio de Budapest sobre ciberdelincuencia adoptado el año 2001 y sus Protocolos complementarios posteriores.

Para apoyar la participación de parlamentarios chilenos en dicha actividad, la presente Minuta contiene una breve descripción del referido convenio, así como de sus protocolos adicionales.

2. Contenido general del Convenio de Budapest

En materia de prevención y sanción del cibercrimen resulta destacable el trabajo que viene desarrollando desde el año 2001 el Consejo de Europa[1], cuando su Comité de Ministros, el día 23 de noviembre, adopta el Convenio sobre Ciberdelincuencia, también llamado Convenio de Budapest, por la ciudad de su firma, el cual entró en vigor el 01 de julio del año 2004.[2]

Dicho instrumento, que se encuentra abierto a la firma tanto de los Estados que integran el Consejo de Europa como de Estados no miembros que hayan participado en su elaboración, y a la adhesión de otros Estados no miembros[3], cuenta a la fecha con la ratificación de 68 de ellos entre los cuales se encuentra nuestro país[4]. En efecto, el Convenio de Budapest fue ratificado por el Congreso Nacional el año 2017 encontrándose vigente a la fecha mediante el Decreto N° 83 de 2017 del Ministerio de Relaciones Exteriores.[5]

El principal objeto de este Convenio, ha sido alcanzar una política penal común que proteja a la sociedad, en general frente a la ciberdelincuencia.

---

[1] Se debe recordar que este es un organismo de carácter regional, que reúne a 46 Estados de Europa, y tiene por principal objeto promover la democracia, los derechos humanos y el Estado de derecho en Europa y el mundo. Todo ello en base a los principios del *Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales*, adoptado en la ciudad de Roma en noviembre de 1950. Para mayor información, véase: https://www.coe.int/es/web/portal/home

[2] ETS N° 185 Convention on Cybercrimen. Disponible en: https://rm.coe.int/1680081561

[3] Conforme dispone el propio Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados contratantes del Convenio y su consentimiento unánime, podrá invitar adherirse al mismo a cualquier Estado que no sea miembro del Consejo de Europa y no haya participado en la elaboración de este instrumento.

[4] Véase: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185

[5] Decreto N° 83 de 2017, Ministerio de Relaciones Exteriores, promulga el Convenio sobre la ciberdelincuencia. Publicado en Diario Oficial de 28 de agosto de 2017. Disponible en: https://bcn.cl/2ij3n

Para ello se promueve no solo la adopción de una legislación adecuada, sino también impulsar mecanismos de cooperación internacional necesarios.

Respecto del marco nacional el Convenio insta a los Estados a la tipificación, en el ámbito de su derecho penal sustantivo, de una serie de conductas consideradas como delictivas (Véase Tabla 1)

Tabla 1. Conductas que deben tipificarse por cada Estado Parte del Convenio.

MEDIDAS A NIVEL NACIONAL: DERECHO PENAL SUSTANTIVO. CONDUCTAS A TIPIFICAR		
Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos	*Acceso ilícito*	Acceso deliberado e ilegítimo a todo o parte de un sistema informático.
	Interceptación ilícita	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.
	Ataques a la integridad de los datos	Todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
	Ataques a la integridad del sistema	Obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
	Abuso de los dispositivos	Comisión deliberada e ilegítima de actos: a) de producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de los delitos señalados en las celdas anteriores; ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer los delitos señalados en la celdas anteriores. b) posesión de algunos de los elementos contemplados en i) o ii) del apartado a) con intención de que sean utilizados para cometer cualquiera de los delitos previstos en las celdas anteriores.

Delitos informáticos	*Falsificación informática*	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.
	Fraude informático	Actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.
Delitos relacionados con el contenido	*Delitos relacionados con la pornografía infantil*	Comisión deliberada e ilegítima de los siguientes actos: a) producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b) oferta o puesta a disposición de pornografía infantil a través de un sistema informático; c) difusión o transmisión de pornografía infantil a través de un sistema informático; d) adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; e) posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.[6]
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines	*Delitos relacionados con infracciones de la propiedad intelectual y derechos afines*	Infracciones de la propiedad intelectual que defina su legislación, conforme obligaciones contraídas en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derechos de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
		Infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artista Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

[6] El Convenio entiende por *pornografía infantil* todo material pornográfico que contenga la representación visual de: a) un menor adoptando un comportamiento sexualmente explícito; b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito; c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito. Asimismo, entiende por *menor* a toda persona de menos de 18 años.

El Convenio insta de igual forma a los Estados Parte a tomar las medidas legislativas, u otras necesarias, para tipificar la complicidad deliberada en la comisión de los delitos detallados, así como la tentativa de cometer los mismos.

De igual forma, llama a adoptar medidas que permitan hacer exigible la responsabilidad de las personas jurídicas por los delitos previstos en la Convención, cuando éstos sean cometidos por cuenta de las mismas por una persona física, a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas, por: a) un poder de representación; b) una autorización para adoptar decisiones en su nombre; c) una autorización para ejercer funciones de control en el seno de dicha institución. Los exhorta además, respecto de estas personas, a responsabilizarlas cuando la ausencia de vigilancia o control de cualquier persona física que ejerza las referidas funciones en una persona jurídica haya permitido la comisión de alguno de los delitos previstos en la Convención por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad. La responsabilidad exigible a las personas jurídicas podrá ser penal, civil o administrativa y no obstará a la responsabilidad penal que recaiga sobre la persona física que cometa el delito.

Las sanciones a aplicar para castigar los delitos aludidos deberán ser efectivas, proporcionadas y disuasorias, incluso tratándose de delitos cometidos por personas jurídicas.

El Convenio expone de manera detallada y en el ámbito del derecho procesal, los procedimientos y poderes, que a través de medidas legislativas o de otro tipo, habrán de adoptar los Estados Parte, para investigar y perseguir los delitos a que la misma refiere; cualquier otro delito cometido por medio de un sistema informático; y para la obtención de pruebas electrónicas de cualquier delito. De este modo, dispone de la necesidad de regulación de aspectos relativos a la conservación y revelación de datos informáticos almacenados, la presentación de los mismos, su registro, confiscación, obtención en tiempo real e interceptación.

Respecto de la jurisdicción para conocer y juzgar estos ilícitos dispone que cada Estado Parte adopte las medidas que la afirmen, cuando el delito se haya cometido: a) en su territorio; o b) a bordo de un buque que enarbole su pabellón; o c) a bordo de una aeronave matriculada según sus leyes; o d) por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar de su comisión o si ningún Estado tiene competencia territorial respecto del mismo. Resuelve además el Convenio, eventuales conflictos de jurisdicción cuando varias Partes se la reivindiquen respecto de un presunto delito.

En lo que refiere a la cooperación internacional, el Convenio dispone de manera textual:

> "Los Estados Parte cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en

> materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos" (artículo 23).

Dispone en este sentido entre otros, reglas relativas a la extradición, a la asistencia mutua en diversas materias (como acceso a datos almacenados, obtención en tiempo real de datos, interceptación de datos, conservación y revelación de datos, etc.), y a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables. Incluso, el Convenio regula la designación por cada Estado Parte de un punto de contacto localizable las 24 horas del día, los 7 días de la semana, a fin de garantizar asistencia inmediata a investigaciones relativas a delitos relacionados con sistemas o datos informáticos o para la obtención de pruebas en formato electrónico de un delito, debiendo disponerse de equipamiento y personal formado a objeto de facilitar su funcionamiento.

3. Protocolos complementarios

El 28 de enero de 2003, en la ciudad de Estrasburgo, se abrió a la firma un primer protocolo complementario al Convenio de Budapest por el cual se persigue la criminalización de los actos de naturaleza racista o xenófoba cometidos a través de sistemas informáticos (ETS N°189).[7]

Este instrumento entró en vigencia el 1 de marzo de 2006 y a la fecha cuenta con la ratificación de 35 Estados. El mismo insta a la tipificación y sanción de conductas efectuadas a través de sistemas computacionales y que consistan, entre otras, en la diseminación de material racista o xenófobo, en amenazas e insultos motivados por racismo y xenofobia, o en la negación, significativa minimización, aprobación o justificación de genocidios o crímenes contra la humanidad.

Este primer protocolo adicional al Convenio de Budapest no ha sido firmado a la fecha por nuestro país.

Finalmente, el 12 de mayo del año 2022 también en la ciudad de Estrasburgo, se abrió a la firma un segundo protocolo complementario al Convenio de 2001 esta vez referido a la cooperación reforzada y a la divulgación de pruebas electrónicas (ETS N° 224), instrumento que requiere

[7] ETS N° 189 Additional Protocol to the Convention on cybercrimen, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Disponible en: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

de 5 ratificaciones para su entrada en vigor (a la fecha solo cuenta con dos). Chile participó de la firma de este instrumento.[8]

Este nuevo protocolo, en atención a la proliferación y complejidad que ha adquirido el ciberdelito, lo que dificulta su persecución, busca otorgar una base legal que permita la divulgación de información de registro de nombres de dominio, la cooperación directa con proveedores de servicios para acceder a información de suscriptores y datos de tráfico, y la cooperación inmediata en caso de emergencia.

[8] ETS N° 224 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Disponible en: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224