LEY MODELO

SOBRE DELITOS INFORMÁTICOS

ÍNDICE

LEY MODELO SOBRE DELITOS INFORMÁTICOS

EXPOSICION DE MOTIVOS

El presente Proyecto de Ley Modelo se plantea realizar las adecuaciones, modificaciones e incorporaciones necesarias a la Ley Marco sobre Ciberdelincuencia aprobada por el Parlamento Latinoamericano y Caribeño en el año 2013, generando una nueva ley modelo circunscripta a la época que vivimos, en la que la tecnología evoluciona a un ritmo muy rápido, y los delitos mutan y se perfeccionan día a día.

En líneas generales, al hablar de delitos informáticos nos referimos a aquellas conductas indebidas e ilegales en las que interviene un dispositivo informático como medio para cometer un delito o como fin u objeto del mismo. Los delitos informáticos son entendidos respecto al lugar que ocupa la tecnología para la comisión del hecho ilícito más que a la naturaleza delictiva del acto mismo, ya que casi todos los delitos contemplados en los ordenamientos jurídicos locales pueden cometerse a través de un dispositivo informático.

En base a ello, se incorpora como objeto del presente Proyecto la regulación de los mecanismos que garanticen la prevención, investigación y sanción de todo acto considerado cibercrimen.

Se propone un cambio de paradigma en la materia y la normativa existente en este ámbito, la cual sólo apuntaba a la criminalización e imposición de penas para los autores de los delitos allí establecidos o que se buscaban establecer en las legislaciones internas. A tal fin se implementa como objetivo central “la prevención ciudadana”, específicamente orientada a niños, niñas y adolescentes, y en general a los sectores de la población más susceptibles de ser víctimas de la ciberdelincuencia.

Se promueve, en igual sentido, la incorporación de planes y programas de cooperación a través de los Parlamentos Miembros del Parlatino basados en un esquema de colaboración públicoprivada, no sólo en materia de lo que podemos denominar “de fondo” sino también “de forma”. Se proponen nuevos delitos como así también métodos o herramientas de cooperación probatoria y procedimental como una cuestión fundamental en este tema.

Se introducen nuevos conceptos que ayudan a hacer completa la modificación propuesta y se redefinen conceptos ya existentes adecuándolos a la actualidad y a la normativa internacional específica, como la Convención de Budapest, logrando, de esta manera, coherencia normativa.

Finalmente, se propone la modificación de las conductas descriptas como delitos y se incorporan nuevas figuras delictivas, actualizando el accionar delictivo que se va perfeccionando para no ser alcanzadas por las normas y ello impone el desafío de ir readecuando las herramientas procesales para su persecución y sanción.

Se busca dar autonomía a conductas que, actualmente no se encuentran contempladas en la normativa, y consecuentemente son encuadradas en delitos que al momento de ser creados no contemplaron la posibilidad de ser cometidos a través de medios informáticos. Por eso, se

presentan dificultades a la hora de querer encuadrar conductas modernas, para aquellos que tienen a su cargo instar un proceso de investigación judicial.

Así, se propone sancionar aquellas conductas relacionadas a la pornografía infantil destacando inclusive la mera tenencia, conductas relacionadas con delitos transnacionales de enorme gravedad tales como la trata de personas y el narcotráfico.

Los medios comisivos utilizados son distintos y mutan constantemente. Las formas de recabar prueba quedan frecuentemente obsoletas, y las herramientas de pruebas muchas veces dependen de normativas internas y de la cooperación entre los Estados.

Por lo expuesto, el presente Proyecto de Ley Modelo busca, a través del Parlatino como espacio de integración regional que permite armonizar respuestas o soluciones conjuntas ante temas que requieren de la intervención de los actores fundamentales del sistema internacional, alcanzar una adecuación normativa capaz de combatir de manera efectiva los delitos informáticos.

LEY MODELO SOBRE DELITOS INFORMÁTICOS

CAPÍTULO I

DISPOSICIONES PRELIMINARES

Artículo 1.- Objeto. La presente Ley tiene como objeto general la regulación de los mecanismos que garanticen la prevención, investigación y sanción de todo acto considerado cibercrimen.

Esta Ley establece, igualmente, las bases normativas para promover la educación de los usuarios y consumidores de sistemas informáticos, como así también la cooperación y asistencia multisectorial, intergubernamental e internacional en la lucha contra los delitos informáticos.

A estos fines las autoridades competentes procurarán la aplicación armónica de esta Ley con otros instrumentos normativos internos e internacionales que establezcan otros delitos y soluciones específicas a éstos, así como mecanismos adicionales de cooperación, asistencia e investigación interna e internacional.

Artículo 2.- Objetivos. Para garantizar el cumplimiento del objeto de la presente Ley, las autoridades competentes procurarán:

a. Prevenir a la ciudadanía en materia de delitos informáticos a través de la conformación de programas educativos y de aumento de capacidades técnicas de los usuarios y consumidores de los sistemas informáticos, como así también la creación de guías sobre buen uso de los servicios informáticos y redes sociales. En el marco de la presente, se deberá poner énfasis y especial cuidado en niños, niñas y adolescentes y en personas jurídicas que no dispongan de los recursos suficientes para adquirir sistemas de informáticos de control y monitoreo acordes a su actividad.

b. Coordinar con los actores del ecosistema digital procesos para garantizar el establecimiento de medidas y programas preventivos a fin de combatir los delitos informáticos.

c. Contribuir al adecuado control y resguardo de la seguridad de la información, propiciando que los sectores sujetos a ataques informáticos cuenten con estructuras tecnológicas que aseguren la confidencialidad, disponibilidad e integridad de la información.

d. Promover planes y programas de cooperación público-privada tendientes a:

1. Poner fin a las acciones maliciosas que tengan por objeto causar daños, provocar pérdidas o impedir el funcionamiento de sistemas informáticos, redes sociales o servicios de internet.
2. Lograr la cooperación efectiva entre los países de la región en materia de seguridad informática y prevención de los delitos informáticos como así también entre éstos y los servidores y proveedores de internet, asimismo los creadores y administradores de redes sociales o aplicaciones de descarga pública o privada.
3. Erradicar las acciones que atenten contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de los mismos.
4. Prevenir, erradicar y sancionar todo hecho delictivo cometido a través de la utilización de sistemas informáticos, internet, redes sociales o servicios de datos, y en general de las distintas actividades que pueden hacer uso de las nuevas tecnologías.

Artículo 3.- Definiciones. Para los efectos de esta Ley, se entenderá como:

a) Abuso Informático de Dispositivos: la producción, venta, obtención para su utilización, importación, difusión u otra forma de cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en esta ley.
b) Ataque Informático: todo intento de exponer, alterar, desestabilizar, destruir, eliminar para obtener acceso sin autorización o utilizar un activo. Será también considerado como tal, cualquier maniobra ofensiva de explotación deliberada que tenga como objetivo tomar el control, desestabilizar o dañar un sistema. En este tipo de ataque el Sujeto Activo es un individuo u organización que intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos, robo de información o de hacer daño a su objetivo.
c) Cibercrimen/Ciberdelincuencia: conjunto de acciones cometidas a través de un bien o sistema informático cuya consecuencia final recae en un hecho considerado como ilícito. Se trata de una vertiente del crimen tradicional que utiliza las nuevas tecnologías para extenderse y desarrollarse de manera exponencial.
d) Datos Informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

e) Datos Relativos al Tráfico: todo dato relativo a una cadena de comunicación que indiquen el origen, destino y ruta de la comunicación o tipo de servicio.

f) Delitos Informáticos: los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes o datos informáticos, así como el abuso de dichos sistemas, redes o datos.

g) Ecosistema digital: es el ambiente creado a través de internet, que esta constituido por el sitio web, el marketin de contenidos, motores de búsqueda, redes sociales y los sistemas de vinculacion digital.

h) Proveedor de Servicios: toda entidad que ofrezca a los usuarios de servicios digitales la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.

i) Sistema Informático: todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan la ejecución de un programa.

Artículo 4.- Partes Que Componen El Delito. A los efectos de la presente Ley, los delitos informáticos se componen de un sujeto activo que será la persona humana o jurídica que realiza el hecho delictivo, y un sujeto pasivo que será aquella persona humana o jurídica lesionada por el mismo.

Respecto de las Personas Jurídicas como sujetos activos, se atribuirá responsabilidad penal cuando los delitos previstos en la presente ley, sean cometidos por una persona humana o jurídica que ejerza funciones directivas en su seno, en virtud de un poder de representación, una autorización para tomar decisiones o una autorización para ejercer funciones de control.

CAPÍTULO II

DELITOS INFORMÁTICOS

Artículo 5.- Conductas Tipificadas: Se entenderá como delito informático la realización de las siguientes conductas:

a) El acceso deliberado e ilegítimo a un sistema informático;

b) Toda manipulación que dañe, elimine, deteriore, altere o suprima datos informáticos;

c) La obstaculización grave del funcionamiento de un sistema informático; o

d) Todo delito cometido contra las personas físicas o jurídicas a través de la utilización de sistemas informáticos, redes sociales, sistemas de datos o aplicaciones de descarga pública o privada.

CAPÍTULO III

DELITOS AUTÓNOMOS

Artículo 6.- Conductas Tipificadas: Se entenderán como Delitos Autónomos los siguientes:

a) Delito informático contra la Propiedad: Aquel que se comete con el ánimo de obtener un beneficio económico, directo o indirecto, y sin autorización expresa del titular de los derechos a través de un medio informático. Entre las conductas que configuran el presente delito se destacan:

1. Editar, reproducir o fijar en cualquier soporte físico o virtual, una obra, interpretación o fonograma.
2. Ofrecer, exhibir, poner en venta, vender, almacenar, distribuir, importar, exportar o de cualquier otro modo comercializar copias ilícitas de obras, interpretaciones o fonogramas, cualquiera sea el soporte utilizado.
3. Incluir a sabiendas información falsa en una declaración destinada a la administración de los derechos de autor o derechos conexos, de modo que pueda ocasionar perjuicio al titular de derechos correspondiente o un beneficio injustificado para el infractor o para un tercero.
4. Alterar, suprimir o inutilizar cualquier medida tecnológica o archivo electrónico que registre información sobre los derechos de autor y derechos conexos, de modo que pueda ocasionar perjuicio al titular de derechos correspondiente o un beneficio injustificado para el infractor o para un tercero.
5. Poner a disposición del público obras, interpretaciones, fonogramas o emisiones de organismos de radiodifusión a través de un sistema informático, o almacenar, efectuar hospedaje de contenidos, reproducirlos o distribuirlos. La misma pena se impondrá, al proveedor de servicios de internet que, teniendo conocimiento efectivo de la falta de autorización, continuare permitiendo el uso de su sistema informático para la comisión de las conductas descritas en este inciso.
6. Realizar hechos dirigidos a sustituir de forma fraudulenta la identidad de una persona o entidad con el objeto de adueñarse de forma indebida de datos confidenciales de acceso y

contraseñas de los usuarios para, lograr deteriorar o desprestigiar su imagen o apropiarse de su patrimonio.

7. Realizar hechos violando medidas de seguridad, e ilegítimamente apoderarse o copiar información contenida en dispositivos o sistemas informáticos ajenos que no esté disponible públicamente y que tengan valor comercial para su titular o para terceros.

b) Delito informático contra la integridad sexual: Aquel que se comete contra la libertad y voluntad sexual de una persona atentando contra su integridad, privacidad e identidad. En el marco del objeto de la presente Ley se entenderán como conductas que configuran el presente delito a aquellas que provocan el atentado descrito a través del uso de los sistemas informáticos, redes sociales, servicios de datos o aplicaciones de descarga pública o privada entre los que se destacan:

1. Producir, financiar, ofrecer, comerciar, publicar, facilitar, divulgar o distribuir por cualquier medio informático, toda representación de una persona menor de DIECIOCHO (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales.

2. Tener a sabiendas en su poder representaciones de las descritas en el párrafo precedente cualquiera sea su fin.

3. Facilitar el acceso a espectáculos pornográficos o suministrar material pornográfico a menores de catorce (14) años.

4. Contactar con una persona menor de edad a través de tecnologías de la información y la comunicación con el fin de cometer delitos sexuales.

5. Obtener fotos o videos de la persona menor de edad en actividades sexuales explícitas o mostrando sus partes genitales o desnudo a través de tecnologías de la información y la comunicación.

6. Fabricar, producir, reproducir, comercializar, difundir o exhibir material pornográfico en el que no habiendo sido utilizados directamente personas menores de edad, emplee la imagen alterada o modificada, caricatura, dibujo o cualquier otra representación visual o la voz de una persona menor de edad, realizando actividades sexuales explícitas, o mostrando sus partes genitales o desnudos.

7. Difundir, revelar, enviar, distribuir o de cualquier otro modo poner a disposición de terceros, sin autorización de la persona afectada, imágenes o grabaciones de audio o audiovisuales de naturaleza sexual, producidas en un ámbito de intimidad, que el autor hubiera recibido u obtenido con el consentimiento de la persona afectada, si la divulgación menoscabare gravemente su privacidad.

8. Publicar o difundir imágenes de desnudez total o parcial y/o videos de contenido sexual o erótico de una o más personas, por medio de comunicaciones electrónicas, telecomunicaciones, o cualquier otro medio o tecnología de transmisión de datos, que se encuentren en posesión de una persona y sean publicadas o difundidas sin el expreso consentimiento de las mismas, aun habiendo existido acuerdo entre las partes involucradas para la obtención o suministro de esas imágenes o video.

c) Delito informático Contra la Identidad Virtual: Aquel que por cualquier acto suplante la identidad de una persona humana o jurídica de forma inequívoca en cualquiera red social, sitio de Internet, medio electrónico o tecnológico de información y transmisión de datos.

d) Delito contra la Seguridad Informática: Aquel que en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

e) Ciberbullying: Todo hecho de abuso psicológico y de acoso llevado a cabo por niñas, niños y adolescentes, contra otros, por intermedio de amenazas, hostigamientos, humillación, chantajes o insultos realizados desde las redes sociales, teléfonos móviles y cualquier otra plataforma digital de comunicación.

f) Phishing: Toda actividad dirigida a sustituir de forma fraudulenta la identidad de una persona o entidad con el objeto de adueñarse de forma indebida de datos confidenciales de acceso y contraseñas de los usuarios con el fin de lograr deteriorar o desprestigiar su imagen o apropiarse de su patrimonio.

Conducta típica a través de la cual el sujeto activo, consigue información de datos de una persona humana o jurídica mediante artimañas fraudulentas, llevándose a cabo mediante un mensaje enviado por correo electrónico o por cualquier aplicación que permita recibir y enviar mensajes o por la suplantación de un acceso mediante una página web falsa o simulada, procediendo con posterioridad a la estafa con apropiación del patrimonio o sustitución de la identidad ajena.

CAPÍTULO IV

COOPERACIÓN INTERNACIONAL

Artículo 7.- Principios Generales y Medidas de Cooperación.

De conformidad con las disposiciones de la presente Ley y de los instrumentos internacionales y regionales pertinentes, las autoridades competentes promoverán la cooperación y asistencia multisectorial, intergubernamental e internacional con sustento en legislaciones uniformes o recíprocas y en la armonización de su derecho interno, con el fin de:

a. Prevenir y combatir los delitos informáticos.

b. Proteger y asistir a la persona humana o jurídica que se ve afectada por la comisión de estos delitos;

c. Llevar a cabo investigaciones y actuaciones en relación con los delitos tipificados con arreglo a la presente ley.

Artículo 8.- Acceso a la justicia. Para el cumplimiento de los fines de esta Ley, se adoptarán las medidas necesarias para que las víctimas de un delito tipificado conforme a las disposiciones de la presente y cometido en el territorio de otro país, puedan formular la denuncia ante las autoridades competentes de su lugar de residencia y tener asistencia adecuada.

Artículo 9.- Cooperación Mutua. Constituye un objetivo de la presente ley promover la cooperación pública- privada para la mejor concreción de la prevención, investigación y sanción de todo acto considerado cibercrimen, así como también para implementar programas de información y educación de usuarios y consumidores de servicios informáticos.

Artículo 10.- Acuerdos Bilaterales/Multilaterales. El Gobierno promoverá la celebración de convenios bilaterales y/o multilaterales sobre lo que es materia de la presente ley, con el fin de completar o reforzar las disposiciones de la misma y facilitar la aplicación de los principios que consagra.

CAPÍTULO V

DISPOSICIONES FINALES

Artículo 11.- Relación con otros Instrumentos Internacionales. Esta Ley no afectará a los derechos y obligaciones derivados de las disposiciones de otros instrumentos internacionales en los que el Estado nacional sea o llegue a ser Parte, que contengan disposiciones relativas a las materias reguladas por la presente y que garanticen una

mayor protección y asistencia a las víctimas afectada por la comisión del delito mencionado precedentemente.