ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA
DEPARTAMENTO DE SERVICIOS TÉCNICOS

INFORME JURÍDICO

PROYECTO DE LEY

"APROBACIÓN DE LA ADHESIÓN AL CONVENIO SOBRE LA CIBERDELINCUENCIA"

EXPEDIENTE Nº 18.484

OFICIO Nº ST.292-2012 J

ELABORADO POR

LICDA. ANA CRISTINA MIRANDA CALDERÓN
ASESORA PARLAMENTARIA

SUPERVISADO POR

LICDA. CRISTINA RAMÍREZ CHAVARRÍA
JEFA DE ÁREA

REVISADO POR

LICDA. GLORIA VALERÍN RODRÍGUEZ
DIRECTORA

19, DICIEMBRE, 2012

TABLA DE CONTENIDO

INFORME JURIDICO[1]

"APROBACIÓN DE LA ADHESIÓN AL CONVENIO SOBRE LA CIBERDELINCUENCIA"

EXPEDIENTE Nº 18.484

I.- RESUMEN DEL PROYECTO

La "Aprobación de la Adhesión al Convenio sobre la ciberdelincuencia", es un instrumento jurídico internacional que busca establecer una política penal común destinada a proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de la legislación apropiada y el fomento de la cooperación internacional con Cada Parte del Consejo de Europa y los otros Estados signatarios del Convenio de cita.

En el preámbulo se indica que el 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, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, 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."*

Con la aprobación del presente Convenio se pretende, además dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos.

El proyecto de ley contiene un único artículo, el que hace alusión a que se apruebe, en cada una de sus partes el "Convenio sobre la Ciberdelincuencia", instrumento compuesto por cuatro capítulos referentes a las siguientes temáticas:

- Capítulo I. Terminología –artículo 1-
- Capítulo II. Medidas que deberán adoptarse a nivel nacional -artículos del 2 al 22-
- Capítulo III. Cooperación internacional -artículos del 23 al 35-
- Capítulo IV - Disposiciones finales -artículos del 36 al 48-

II.- CONSIDERACIONES SOBRE EL FONDO DEL PROYECTO

En primer término, previo al análisis de la iniciativa, hemos de indicar que en la corriente legislativa se encuentra en trámite el Proyecto de ley N° 18.546 "Reforma de los tipos penales establecidos en los artículos 167, 196, 196 bis, 231, 236 y 288 del Código Penal, Ley Nº 4573, publicada en el alcance 120 de la gaceta 257 de 15 de noviembre de 1970 y sus reformas", (conocido como ley mordaza). Este expediente

[1] Elaborado por la **Licda. Ana Cristina Miranda Calderón**, **Asesora Parlamentaria**. Supervisado por la **Licda. Cristina Ramírez Chavarría, Jefa de Área.** Supervisión y Aprobación Final a cargo de la **Licda. Gloria Valerín Rodríguez,** Directora Departamento de Servicios Técnicos.

cuenta con Informe del Departamento de Servicios Técnicos, egresado mediante Oficio ST- 263-2012 J, del 26 de noviembre del 2012.

La observación obedece a que el instrumento Internacional aquí analizado Expediente 18.484, *presenta en el Capítulo II una "Sección 1. Derecho Penal Sustantivo", que desarrolla un Título sobre "Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos", entre ellos:* ***"Acceso Ilícito, Interceptación Ilícita, Interferencia en los datos, Interferencia en el Sistema, Abuso de los dispositivos, Falsificación Informática, y Fraude Informático"*** **y** además desarrolla una serie de elementos relativos al contenido de algunos delitos y aspectos de **derecho procesal penal**.

En ese sentido, tal como lo indicáramos la rendir informe sobre el Expediente 18.546, en virtud de que los instrumentos internacionales por disposición del artículo 7 de la Constitución Política tienen autoridad superior a las leyes, esta asesoría considera meritorio que dentro de la dinámica de las Comisiones que tramitan reformas al Capítulo de Delitos Informáticos del Código Penal y la Comisión Especial de Asuntos Internacionales, se considere el contenido e incidencia de los textos en trámite con el propósito de armonizar la legislación y se evite posteriores roces con los tipos penales regulados tanto en el ordenamiento vigente como respecto del contenido que finalmente se implemente al Expediente Nº 18.546 y el Instrumento Internacional aquí analizado bajo el Expediente Nº 18.484.

Aclarado lo anterior y para efectos de abordar el estudio de la presente iniciativa, se considera conveniente recordar algunos aspectos sobre: la Adhesión a un Convenio Internacional, los aspectos más sobresalientes señalados en diferentes foros nacionales sobre el tema de ciberdelincuencia, y una reseña de los elementos que componen el Convenio sobre ciberdelincuencia, lo cuales se desarrollan de seguido.

A. Sobre la adhesión de un Convenio Internacional[2]

En virtud de que con este proyecto de ley, se pretende que nuestro país se **adhiera** a la *"Convenio sobre la ciberdelincuencia",* en los artículos 36 y 37 de éste mismo instrumento internacional, ***se hace referencia a la entrada en vigor de éste convenio para los países que se hayan adherido posteriormente***, es importante destacar lo que la Sala Constitucional[3] ha manifestado sobre el ***procedimiento de adhesión***, a saber:

> *"en atención a lo dispuesto en los artículos 2 y 11 de la Convención de Viena sobre el Derecho de los Tratados (Ley Nº 7615 de 24 de julio de 1996,* ***la adhesión es el acto internacional por el cual un Estado hace constar en el ámbito internacional su consentimiento en obligarse por un tratado que no fue negociado directamente por éste****.* ***Y el artículo 15*** *de la Convención de Viena sobre el Derecho de los Tratados establece, en su inciso a), que* ***el consentimiento de un Estado en obligarse por un tratado se manifiesta mediante la adhesión cuando el propio tratado disponga tal posibilidad.*** *…"* (El resaltado no es del original).

---

[2] Este apartado es tomado del criterio del **Departamento de Servicios Técnicos**, Oficio ST N° 158-2012 J de 9 de agosto del 2012, sobre el expediente Nº 18.382, proyecto de ley: "APROBACIÓN DE LA ADHESIÓN A LA CONVENCIÓN PARA FACILITAR EL ACCESO INTERNACIONAL A LA JUSTICIA".

[3] **Sala Constitucional**. Voto N° 18209-2008 de las 18:17 horas del 10 de diciembre del 2008.

Sobre esta misma materia, agrega en este Voto la Sala Constitucional:

> *"en el caso del citado artículo 11 de la Convención de Viena sobre el Derecho de los Tratados, el Gobierno de Costa Rica hizo la reserva en el sentido de que el sistema jurídico constitucional de* ***nuestro país no autoriza ninguna forma de consentimiento que no esté sujeto a la ratificación de la Asamblea Legislativa.*** *Ello en atención a lo dispuesto en el inciso 4), del artículo 121 de la Constitución Política, que establece que corresponde, exclusivamente, a la Asamblea Legislativa aprobar o improbar los convenios internacionales, tratados públicos y concordatos.* ***Este Tribunal ya se ha pronunciado sobre el procedimiento de adhesión a un instrumento internacional, y ha manifestado que ésta no infringe el Derecho de la Constitución, siempre que conste la voluntad del Poder Ejecutivo de obligarse por dicho instrumento, y que este sea sometido a aprobación del órgano parlamentario."*** *(El resaltado no es del original).*

Por otra parte cabe anotar, que el Departamento de Servicios Técnicos, con ocasión del estudio de un proyecto de ley de la misma naturaleza (**adhesión a un convenio internacional**), enunció: *"Por tratarse de la aprobación de la adhesión de nuestro país a un convenio vigente, no corresponde solicitar ni la suscripción del convenio, ni el otorgamiento de los Plenos Poderes, pues en este caso, la manifestación del Estado de obligarse estaría constituida por la adhesión a este instrumento y tiene los mismos efectos que la ratificación*."[4]

Asimismo, indicó: ***"La adhesión tiene el mismo efecto jurídico que las demás formas mediante las cuales los Estados pueden obligarse por un tratado o acuerdo. En el caso de Costa Rica se requiere la aprobación del proyecto de ley por parte de la Asamblea Legislativa, posterior a ello el Poder Ejecutivo sanciona la ley y se publica en el Diario Oficial "La Gaceta". Y para crear obligaciones jurídicas vinculantes con arreglo al derecho internacional mediante la adhesión solo se requiere el depósito del instrumento.*** *(…)"*[5]

Como se determina, en el caso en estudio se reúnen los requisitos señalados en el inciso a) del artículo 15 de la Convención de Viena sobre el Derecho de los Tratados, que indica que **el consentimiento de un Estado en obligarse por un tratado se manifiesta mediante la adhesión cuando el propio tratado disponga tal posibilidad.** En este sentido dispone:

> ***"15. Consentimiento en obligarse por un tratado manifestado mediante la adhesión.*** *El consentimiento de un Estado en obligarse por un tratado se manifestara mediante la adhesión:*
>
> *a) cuando el tratado disponga que ese Estado puede manifestar tal consentimiento mediante la adhesión: (…)."*

---

[4]Informe Jurídico, sobre el Proyecto de Ley N° 18.320 denominado "Aprobación de la Adhesión al Acuerdo sobre Medidas del Estado Rector del Puerto, Destinadas a Prevenir, Desalentar y Eliminar, la Pesca Ilegal, no Declarada y no Reglamentada." ST-096-2012-I. Realizado por la Licda. Norma Eugenia Zeledón Pérez, asesora jurídica y la Msc. Xinia Escalante, asesora social, supervisado por el Msc Gastón Vargas Rojas, Coordinador del Área Socio-Ambiental. Autorización final del Lic. Freddy Camacho Ortiz, Subdirector a.i., Departamento de Servicios Técnicos.

[5]*Ibid.*

En concordancia con lo señalado en el Convenio de Viena, en el artículo 37 de este convenio internacional en análisis, se establece expresamente la posibilidad de que otros Estados puedan adherirse a éste. En este sentido dispone este artículo:

"Artículo 37 - Adhesión al Convenio

1. *Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d) del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros.*
2. *Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrar· en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa."*

En cuanto a la invitación que debe cursarse por parte del Comité de Ministros del Consejo de Europa, para poder considerarse el Estado de Costa Rica invitado para valorar la adhesión al presente Convenio, en la exposición de motivos del proyecto de ley, se indica que:

"El Comité de Ministros del Consejo de Europa, en el curso de la reunión sostenida a nivel de delegados el 31 de enero de 2007, invitó a Costa Rica a adherirse al Convenio sobre la Ciberdelincuencia hecho en Budapest, el 23 de noviembre de 2001, de conformidad con su artículo 37."

Además, en cuanto al requisito que hace referencia la Sala Constitucional, sobre la procedencia de la adhesión de un instrumento internacional, **"siempre que conste la voluntad del Poder Ejecutivo de obligarse por dicho instrumento, y que este sea sometido a aprobación del órgano parlamentario",** es importante acotar que este proyecto de adhesión al *"Convenio sobre la ciberdelincuencia",* **es una iniciativa del Poder Ejecutivo, suscrita por la Presidenta de la República y el Ministro de Relaciones Exteriores y Culto.**

Por otra parte, en cuanto a la entrada en vigencia del instrumento internacional, es necesario acotar que de conformidad con lo establecido en los artículos 121 inciso 4); 129 y 140 inciso 10) de la Constitución Política, la entrada en vigencia de un tratado internacional, lleva implícito como requisitos internos de consentimiento, el cumplimiento de la aprobación de la Asamblea Legislativa, la ratificación del Poder Ejecutivo y la publicación en el diario oficial. Una vez cumplidos éstos, se sujeta a lo dispuesto por el artículo 37 punto 2 del Convenio en estudio.

B. Sobre elementos de interés acerca de la ciberdelincuencia en distintos foros nacionales

La Adhesión al Convenio sobre la ciberdelincuencia, constituye un instrumento jurídico internacional, que aporta a nuestro ordenamiento jurídico un marco de "leyes-modelo" o "leyes-tipo", lo que implicará las reformas normativas en nuestro derecho interno para armonizarla con los términos indicados en el presente Convenio; estableciéndose una aplicación territorial amplia entre los países Partes del Convenio.

En Costa Rica se ha realizado un esfuerzo de concientización, mediante diferentes foros de discusión, encaminados a estudiar los delitos informáticos, llegando a la conclusión que el desconocimiento que tienen los usuarios de Internet sobre los ataques informáticos, así como los vacíos en la legislación costarricense, facilitan el ser víctima de la ciberdelincuencia. De forma que a continuación se realizará una breve reseña de algunos foros, que indican los elementos esenciales que se han abordado sobre el particular.

Desconocimiento y vacíos legales facilitan la ciberdelincuencia en el país[6]

Actualmente Internet es considerado un mundo enorme y complejo, donde pueden ocurrir delitos informáticos debido a la facilidad con la que se comparten datos e información en tiempo real. A esto se le suma que los usuarios de la red no están conscientes de los peligros a los cuales se exponen, con lo que aumenta el riesgo de ser víctima de un ataque. En la Internet no sólo se puede encontrar software malintencionado, sino que también ocurre la suplantación de identidad, recolección de información privada de redes sociales y ataques multiplataformas. El uso de software sin una licencia del fabricante, también impide que se instalen actualizaciones que protegen la seguridad de los sistemas. Los delitos ya no se limitan a las computadoras, sino que incluyen a todo dispositivo que tenga conexión a Internet como los celulares y las tabletas.[7]

Incluso ese mismo exponente[8] citó el Reporte de Seguridad Informática 2011 de la empresa ESET, el cual indica que en Costa Rica, el 36% de las empresas permite el uso de redes sociales sin ninguna restricción. El 50% de los usuarios costarricenses considera que no hay malware (software malicioso) en dichos sitios, y el 22% agrega como contacto a personas desconocidas. El Dr. Carlos Chinchilla Sandí[9] coincidió que los usuarios creen que no serán víctimas de un ataque cibernético en Internet, especialmente en las redes sociales.

El Dr. Chinchilla[10] señaló que quien comete un delito informático puede ser una persona o un grupo de personas, que manejan información sensible o importante, hasta profesionales especializados en informática. Las personas que delinquen en la red se muestran agradables, amigables y educadas, por lo que la víctima no sospecha que está frente a un ataque informático.

Para comprender el delito informático es necesario conocer las redes informáticas y los equipos informáticos. Un delito como este no se visualiza correctamente si no se

---

[6] Mesa redonda ***"Desconocimiento y vacíos legales facilitan la ciberdelincuencia en el país"***, organizada por la Facultad de Derecho de la Universidad de Costa Rica, en conjunto con el Departamento de Servicios Bibliotecarios, Documentación e Información de la Asamblea Legislativa. Publicada por Universia Noticias Costa Rica, el 05 de octubre de 2011. Sitio: http://noticias.universia.cr/en-portada/noticia/2011/10/05/875040/desconocimiento-vacios-legales-facilitan-ciberdelincuencia-pais.html

[7] Indicado por el Lic. Roberto Lemaitre Picado, miembro del Área de Informática Jurídica de la Facultad de Derecho de la Universidad de Costa Rica.

[8] Ibid.

[9] Exponente de la mesa redonda *"Desconocimiento y vacíos legales facilitan la ciberdelincuencia en el país"*, Magistrado de la Sala III de la Corte Suprema de Justicia, egresado de la UCR y cuenta con publicaciones sobre delitos informáticos y derecho penal.

[10] Ibid.

comprende el ecosistema en el que se desarrolla. Por lo que la persecución y la prueba de un delito informático son complicadas, para ejemplificarlo, el Lic. Lemaitre[11] indicó que un ciberdelincuente puede atacar desde Costa Rica y hacer creer que el delito se cometió en cualquier otro país del mundo, lo que dificulta la captura física del atacante y se requiere de colaboración internacional. Muchas empresas no denuncian que sus sistemas son víctimas de ataques informáticos, por miedo a dañar su imagen y perder la confianza de sus clientes, lo que colabora con la impunidad.

Los especialistas participantes en la mesa redonda[12] coincidieron en que la legislación costarricense presenta serias deficiencias para proteger a la ciudadanía de la ciberdelincuencia, debido a los vacíos conceptuales y la falta de tipos penales para sancionar.

Toda vez que en los sistemas informáticos hay tres fases importantes: el ingreso, procesamiento y salida de información. Y está comprobado estadísticamente, que el 85% de los ataques cibernéticos ocurren en la primera etapa.[13]

Por lo que planteó como otro de los vacíos de la legislación costarricense en materia de ciberdelitos, que sólo se contemplan sanciones a personas físicas, y no a empresas que comentan actos ilícitos, con lo que se facilita el crimen organizado.

El expositor M.Sc. Francisco Salas Ruiz[14] destacó la necesidad de que el país se una al Convenio de Europa sobre ciberdelincuencia. Considera que una vez que el país esté adherido al Convenio, podrá pedir ayuda a otros países que forman Parte de éste para perseguir los delitos informáticos.

Los especialistas de la mesa redonda[15], fueron enfáticos al decir que el derecho informático requiere de un trabajo interdisciplinario que incluya a juristas, especialistas en informática y computación. Una actualización constante en la legislación, tal y cómo lo hace la tecnología. Y la creación en Costa Rica de una institución especializada en el sector judicial que se encargue de investigar los delitos informáticos.

Especialistas reconocen necesidad de ley sobre ciberdelitos*[16]*

Para abordar la temática de los ciberdelitos se establecen dos tendencias: la que **considera los delitos informáticos como conductas novedosas**, en cuyo caso las acciones y los tipos penales son nuevos y múltiples; y la que ve esos **delitos como conductas tradicionales en un contexto moderno**, para los cuales se reforman o agregan leyes existentes.[17]

---

[11] Ibid.
[12] Ibid.
[13] Ibid, indicado por el Dr. Chinchilla.
[14] Ibid, es Procurador del Sistema Nacional de Legislación Vigente, profesor de la Facultad de Derecho de la Universidad de Costa Rica, y ha representado a Costa Rica en diferentes comisiones sobre delitos informáticos fuera del país.
[15] Ibid.
[16] En el foro **Tipo y naturaleza de los ciberdelitos**, fue parte de unas jornadas organizadas por el Programa Sociedad de la Información y el Conocimiento (Prosic) de la Universidad de Costa Rica, publicado en el Boletín Presencia Universitaria, noviembre de 2009, por *Mayela Castillo Villachica*.
[17] Indicado por el exponente Dr. Christian Hess Araya, Juez del Poder Judicial.

En Costa Rica se han utilizado ambas tendencias, en una combinación de reformas y creación de tipos penales, que castigan las acciones delictivas, por ejemplo la creación de los **delitos de fraude electrónico, alteración de datos y sabotaje informático** y la propuesta para reformar artículos del Código Penal, en cuanto a **fraudes de tarjetas de crédito e información bancaria o Ley de Delitos Informáticos**.[18]

La delincuencia informática en Costa Rica se da de dos formas principalmente: **la violación de comunicaciones electrónicas**, por medio del reenvío a cuentas ajenas y robo de claves de acceso a correos electrónicos y por **alteración de datos y sabotaje informático**, como el acceso a entidades públicas, la venta de información confidencial, el daño a la compra de equipos personales y el cambio de saldos de las cuentas bancarias. Además, existen otras formas de delincuencia recurrentes como son: **la producción y difusión de pornografía infantil, el acoso infantil, el robo de identidad, amenazas y extorsiones, estafas, fraudes y ciberterrorismo.[19]**

Se planteó[20] la necesidad de integrar un enfoque judicial a uno educativo en materia de delincuencia informática, ya que no es un tema que se resuelva creando leyes, se requiere educación al público, sobre el uso correcto y seguro de la tecnología.

La educación de los usuarios debe ir dirigida a solucionar la ingenuidad de las personas, enseñarles a no abrir correos de desconocidos, no seguir los vínculos a los sitios web de los bancos e informarse en un vocabulario no técnico ni especializado. Además señaló que el seguro que proteja contra el fraude informático es una necesidad en Costa Rica.[21]

Se reitera en este Foro[22] la necesidad de ser Parte del Convenio Europeo sobre ciberdelincuencia, ya que aporta definiciones sustantivas respecto a los términos utilizados como acciones delictivas, así como las características para su comisión. Además de la inclusión de normas que garantizan la integridad del usuario, el respeto a los derechos de propiedad intelectual, contempla acciones como la falsedad informática y la pornografía infantil, como delitos punibles. La legislación costarricense contiene normativa respecto a algunos de esos aspectos, pero adolece de normativa que garantice el respeto a los derechos de los usuarios.

Por la naturaleza de los delitos informáticos se dificulta su persecución; lo difícil que es identificar la comisión de un delito, identificar al autor o autores de ese delito, perseguirlos, o sea someterlos a la acción de la justicia y, eventualmente, condenarlos.[23] Por lo que d**estaca en la comisión del delito la velocidad con la que se realizan, la distancia geográfica entre los sujetos involucrados debido al medio, que es Internet, la facilidad de encubrir las pruebas, el temor a denunciarlos y el perfil no tradicional del delincuente informático**.

Los delitos informáticos son las violaciones a los derechos de autor, el robo de datos privados, la pornografía infantil y el fraude electrónico, por citar algunos casos, y no

[18] Ibid.
[19] Según lo explica el expositor Lic. Erick Lewis Hernández, jefe de Delitos Informáticos del Organismo de Investigación Judicial.
[20] Dr. Christian Hess Araya.
[21] Licda. Adriana Rojas Rivero, Presidenta de la Asociación de Consumidores Libres.
[22] Por parte del Lic. Francisco Salas Ruiz, Procurador Adjunto de Derechos Informáticos.
[23] Indicado por el Dr. Christian Hess Araya.

aquellos que se cometan sobre artefactos tecnológicos, como sería robar un cajero automático.[24]

Un aspecto fundamental que impide el castigo de los delincuentes informáticos es la indiferencia de la opinión pública, esto porque no se le da trascendencia a este tipo de delitos, como sí se hace a los tradicionales[25]. Otra causa apuntada es el desconocimiento y confusión, generalmente, no se realizan las denuncias correspondientes[26]. Así como el temor al desprestigio y la consecuente pérdida económica, todo lo cual se convierte en una de las más grandes trabas a la penalización de los delitos informáticos.[27]

A continuación se ofrece una breve lista de terminología que se utiliza en los ciberdelitos, veamos:

- ***Delitos informáticos**: Acción delictiva que realiza una persona con la utilización de un medio informático, lesionando los derechos del titular de un elemento informático, ya sean máquinas (hardware) o programas (software).*
- ***Virus informático**: programa que tiene por objetivo alterar el funcionamiento normal del equipo de cómputo, sin autorización del usuario.*
- ***Spyware**: programa que se instala en el equipo de cómputo, con el fin de recopilar información sobre las actividades que se realizan en él.*
- ***Phishing**: tipo de estafa que utiliza medios electrónicos e informáticos para obtener información confidencial de forma engañosa, como claves de acceso o información bancaria.*
- ***Pharming**: basado en ingeniería social, la víctima es conducida a un sitio falso para que ceda su información confidencial y luego es redirigida a un sitio falso, con un nombre igual al sitio de destino.*
- ***Keylogger**: programa espía que guarda las teclas presionadas en el teclado y hace que el correo electrónico lleve un archivo que tiene el programa escondido para transmitir las claves.*

Expertos creen que Ley de Delitos Informáticos debe ser equilibrada en aspectos jurídicos y técnicos[28]

La principal conclusión que se llegó en la mesa fue que Costa Rica necesita una legislación sobre delitos informáticos que sea actual y equilibrada en aspectos técnicos y jurídicos para proteger a los usuarios y la información de la ciberdelincuencia.

El país necesitaba una nueva ley de delitos informáticos, pues **la sociedad costarricense cada vez más tiene acceso a las nuevas tecnologías con lo cual exponen su información e identidad** en diferentes redes locales y globales gracias a Internet. La última legislación vigente en esta materia era del 2001.[29]

---

[24] Manifestaciones de Licda. Adriana Rojas Rivero.
[25] Opinión del Dr. Christian Hess Araya.
[26] Criterio de la Licda. Adriana Rojas Rivero.
[27] Opinión del Dr. Carlos Chinchilla.
[28] Mesa redonda *"Reflexiones en torno a la nueva Ley de Seguridad Informática",* organizada recientemente por el Programa Sociedad de la Información y el Conocimiento de la Universidad de Costa Rica (Prosic). Con el objetivo de otorgar un espacio para intercambiar ideas sobre la Ley de Delitos Informáticos Ley N° 9048. Publicación hecha por **Universidad de Costa Rica** en el Boletín N° 21 de agosto de 2012, Categoría: Tecnología, por Anna Georgina Velásquez Vásquez.

Con el fin de dar una contextualización se indicó[30] que la sociedad de Costa Rica ha cambiado. Vivimos en lo que ahora denominamos la cibersociedad, que presenta la información como bien y como actividad. **Costa Rica se encuentra entre los primeros 10 países de Latinoamérica que más genera ataques maliciosos hacia la red.** Y la persecución de un delito informático suele ser muy compleja debido a la forma en la que se transmiten los datos y porque **las evidencias son muy sensibles a sufrir cambios**, lo que dificulta delatar al autor de un ataque.

Con la **Ley 9048**[31] **de Delitos Informáticos se establecen reformas al Código Penal**, se adicionan nuevos tipos penales como suplantación de identidad, suplantación de páginas electrónicas e instalación o propagación de programas informáticos maliciosos. Se contemplan otros delitos como la violación de correspondencia y datos personales, extorsión, estafa informática, daño informático y espionaje. Con lo cual se busca la protección de personas físicas y personas jurídicas. Las penas son más altas para las personas que sean encargadas de administrar o dar soporte a un sistema o red informática y comentan un delito, dado su conocimiento técnico y el acceso que poseen a la información.

Los participantes en la actividad coincidieron que la nueva legislación de delitos informáticos presenta reformas importantes en el tema de ciberseguridad, pero también contiene artículos que han causado **polémica y dudas sobre su aplicación.** Además, la velocidad con la que se desarrollan las tecnologías se vuelve un obstáculo para mantener una legislación actualizada y sin vacíos legales.

La formulación y aprobación en Plenario Legislativo de la Ley 9048 de Delitos Informáticos fue **un proceso largo que requirió de la asesoría de técnicos especialistas** en el tema. Incluso, el proyecto de ley fue revisado por un representante del Consejo de Europa, que es la instancia internacional más reconocida que ha dictado estándares a nivel mundial sobre ciberdelincuencia.[32]

Además indicó[33] que el artículo 288 sobre espionaje informático, **no fue formulado con fines políticos o para atentar contra la libertad de expresión y la labor periodística.** Dicho artículo plantea: "Será reprimido con prisión de cuatro a ocho años al que procure u obtenga indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado". Según el especialista, la prensa ha **malinterpretado e**

---

[29] Lic. Roberto Lemaitre Picado, abogado e ingeniero informático.

[30] Lic. Lemaitre.

[31] **Esta Ley se originó mediante la tramitación del Expediente Nº 17.613, *"Reforma al Artículo 229 BIS del Código Penal y Adición de un Nuevo Capítulo denominado: "Delitos Informáticos",* respecto del cual el Departamento de Servicios Técnicos rindió Informe Técnico elaborado por al Licda. Cristina Ramírez Chavarría, conforme Oficio ST. 039-2010-J del 10 de marzo del 2010. Este expediente fue aprobado por el Plenario Legislativo mediante el Decreto de Ley Nº 9048 de 10 de julio de 2012, "REFORMA DE VARIOS ARTÍCULOS Y MODIFICACIÓN DE LA SECCIÓN VIII, DENOMINADA DELITOS INFORMÁTICOS Y CONEXOS, DEL TÍTULO VII DEL CÓDIGO PENAL", publicada en la Gaceta Nº 214, alcance 172 del 6 de noviembre de 2012. Cabe indicar que no todas las recomendaciones técnicas fueron implementadas.**

[32] El M.Sc. Francisco Salas Ruiz, abogado especialista en delitos informáticos y profesor de la Facultad de Derecho de la Universidad de Costa Rica.

[33] Ibid.

incomprendido la legislación y no ha consultado la opinión experta de los técnicos que ayudaron a redactar la ley. Tampoco se ha tomado en cuenta que la figura de informaciones secretas políticas está contemplada en el Código Penal desde 1970.

"Esto es un trabajo bastante técnico. No será perfecto, por supuesto que no, pero yo creo que las personas que hemos participado, quienes lo han revisado y le han dado el visto bueno, son personas que tienen absolutamente toda la credibilidad en esta materia, porque es sumamente especializada. No se trata de un tema político".[34]

El abogado[35] manifestó que **el delito de espionaje se configura en el momento en el que se da la apropiación de la información**, por lo que no se coarta la libertad de expresión, porque **no es necesario revelar ciertos datos para cometer un delito**.

En contraposición a lo indicado, se señaló[36] que la **ley de delitos informáticos es necesaria**, **pero requiere cambios importantes**, ya que en varios apartados no solamente tiene afectación para los periodistas, sino para los comunicadores, que pueden ser todos y todas. Se cuestionó que si ninguna persona ha sido acusada por la obtención de informaciones secretas políticas, ¿por qué es necesario mantener ese término en la ley?, este hecho no descarta que en el futuro alguien pueda ser sancionado. Costa Rica es un país democrático donde **el uso de los secretos de Estado debería ser limitado para asegurar la transparencia política**. Además, la Ley de Delitos Informáticos debería armonizar el término de informaciones secretas políticas con el de secretos de Estado que se presenta en la Constitución Política. *"A mí me preocupa muchísimo que al final una interpretación que hacen los comunicadores al respecto de la ley, permita que nosotros apliquemos una autocensura y un temor a seguir investigando sobre temas específicos en el caso que caigan en esas tres palabras (informaciones secretas políticas)".*

Para combatir la ciberdelincuencia de forma efectiva, los especialistas coincidieron en que es necesaria la **educación del usuario** y la **voluntad política** para emitir una legislación equilibrada en lo técnico y lo jurídico.

La educación es necesaria para asegurar la protección de los usuarios y su información, pues no basta con tener una ley. *"Generalmente la principal vulnerabilidad de un sistema informático viene a ser la falta de conocimiento que tienen los mismos usuarios de las nuevas tecnologías o de las tecnologías en general"*.[37]

Siguiendo la misma línea de pensamiento, se indicó[38] que los usuarios suelen ignorar de la **importancia de actualizar los programas antivirus y los equipos** para disminuir vulnerabilidades. Además, la **formación jurídica e informática** también debe incluir a los abogados y jueces para comprender mejor los delitos y aplicar la justicia. *"Los jueces y abogados ocupan formarse en términos técnicos también para que comprendan este tipo de delitos. Si sólo se mantienen en el tema jurídico no van a comprender cómo ocurren estos delitos, qué es lo que hay detrás"*.

---

[34] Ibid.
[35] Ibid.
[36] Dr. Marlon Mora, periodista, académico y representante del Colegio de Periodistas (Colper).
[37] El Lic. José Adalid Medrano, abogado y consultor sobre ciberdelincuencia.
[38] Lic. Lemaitre.

Por último, se consideró[39] que la voluntad política es clave para lograr una legislación contra la ciberdelincuencia efectiva. En la tramitación de la Ley N° 9048 de Delitos Informáticos, **los asesores legislativos ignoraron recomendaciones** que hicieron los técnicos especialistas y eso se traduce en **errores y vacíos legales**. Por ejemplo, es necesario que se contemple en la ley **la colaboración transfronteriza** para que los delitos informáticos no queden impunes, pues la ciberdelincuencia es una realidad mundial que no se limita a Costa Rica.

En la mesa redonda se comentó a manera de conclusión final, que se ha presentado en la corriente legislativa un **proyecto de ley[40]** , que pretende corregir los **vicios y vacíos legales** que se considera tiene la Ley N° 9048 de Delitos Informáticos.

En este informe jurídico, en el apartado de sobre "Anexo", a modo de referencia, se presenta un cuadro comparativo entre la Ley 9048 "Reforma de varios artículos y modificación de la Sección VIII, denominada Delitos Informáticos y conexos, al Título VII del Código Penal, y reforma del artículo 9 de la Ley Nº 7425", expediente 18546 "Reforma de los tipos penales establecidos en los artículos 167, 196, 196 bis, 231, 236 y 288 del Código Penal, Ley Nº 4573, publicada en el Alcance 120 de La Gaceta 257 de 15 de noviembre de 1970 y sus reformas y el "Código Penal, Ley Nº 4573, de 4 de mayo de 1970 y sus reformas"; con el objetivo de observar la evolución de la regulación de las conductas que se han tipificado en nuestro derecho interno.

Sin embargo, esta normativa no contempla o tipifica otras figuras y actos que son importantes de rescatar y analizar en el ámbito de derecho penal, procesal y la cooperación internacional, los cuales son tratados en el Convenio en estudio. Por lo que en el apartado de "Análisis del articulado" se especifican dichas conductas, entre otros aspectos.

Comentario de opinión acerca de la Adhesión al Convenio Europeo sobre Ciberdelincuencia [41]

"Este tratado internacional, firmado en Budapest el 23 de noviembre de 2001, es el primer instrumento multinacional diseñado para combatir el problema de los delitos informáticos. Posteriormente, en el 2003, se promulgó un Protocolo Adicional para reprimir actos de racismo y xenofobia cometidos por medios tecnológicos.

El CEC surgió del convencimiento de que el carácter transnacional de los delitos cometidos por medio de la Internet exige la adopción de un instrumento jurídico que permita su prevención y represión exitosas, por medio de medidas legales y procedimientos que mejoren la cooperación internacional en esta materia.

---

[39] Por parte del El Lic. Medrano

[40] En este sentido se recomienda analizar las observaciones hechas por el **Departamento de Servicios Técnicos**, ST- 263-2012 J, 26 de noviembre, 2012 sobre el proyecto de ley N° 18546 *"Reforma de los tipos penales establecidos en los artículos 167, 196, 196 bis, 231, 236 y 288 del Código Penal, Ley Nº 4573, publicada en el alcance 120 de la gaceta 257 de 15 de noviembre de 1970 y sus reformas".*

[41] **La Nación.** Artículo de Opinión "Adhesión al Convenio Europeo sobre Ciberdelincuencia", Christian Hess Araya, publicado el jueves 29 de noviembre del 2012.

El Convenio no solo cubre aspectos de derecho penal sustantivo sino también procesal, incluyendo la territorialidad, los mecanismos de cooperación mutua y la extradición.

El Convenio comprende una serie de estándares mínimos para los Estados parte. Esto significa que cada cual puede decidir si desea aplicar políticas más severas en relación con la materia. Se identifican nueve delitos agrupados dentro de cuatro categorías:

a) Delitos relacionados con el contenido. Por ejemplo, producir o difundir pornografía infantil.
b) Delitos relacionados con infracciones a la propiedad intelectual y los derechos afines. Ejemplo: copiar y distribuir programas de software propietario (piratería informática).
c) Delitos informáticos, incluyendo el fraude y la falsificación informática. Ejemplo: borrar de modo fraudulento la información de una base de datos.
d) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, incluyendo el acceso ilícito a sistemas informáticos, la interceptación ilícita de datos informáticos, la interferencia en el funcionamiento de un sistema informático y el abuso de dispositivos que faciliten la comisión de delitos. Ejemplos de ello serían el robo de identidad y la implantación de virus o de keyloggers.

De concretarse nuestra adhesión al CEC, sería necesario ajustar la legislación penal nacional a fin de compatibilizarla plenamente con estas disposiciones del convenio.

Finalmente, valga notar que el interés de llevar a cabo esta adhesión no es reciente.

Ya en 2004, el Gobierno del entonces presidente Abel Pacheco solicitó a la Cancillería explorar los procedimientos para lograrlo (puede verse al respecto el oficio Nº 162-05-OAT-PE de 5 de mayo de ese año de la Dirección General de Política Exterior). Luego, en el 2007, algunos legisladores –incluyendo a la entonces diputada Ana Helena Chacón– retomaron la iniciativa, que fue vista con buenos ojos por la ministra de Justicia y actual presidenta Laura Chinchilla."

De lo analizado en todos los foros, observamos como punto de encuentro que todos los especialistas consideran como necesidad que Costa Rica sea Parte del Convenio Europeo sobre ciberdelincuencia.

Precisamente, por el carácter transnacional de los delitos informáticos, lo que exige la adopción de medidas preventivas y represivas exitosas. Para ello, se requiere ajustar la legislación penal nacional, a fin de compatibilizarla plenamente con las disposiciones del Convenio. De esa manera se protegerá a los usuarios y la información de la ciberdelincuencia, mejorando la cooperación internacional en esta materia.

Además, se concluye que para combatir la ciberdelincuencia de forma efectiva, es necesaria la **educación del usuario** para asegurar la protección de los usuarios y su información, y la **voluntad política** para emitir una legislación equilibrada en lo técnico y lo jurídico.

Se concientiza sobre el trabajo interdisciplinario - juristas, especialistas en informática y computación- que requiere el derecho informático. Así como la actualización constante en la legislación, cómo lo hace la tecnología.

III.- ANÁLISIS DEL ARTICULADO DEL CONVENIO

Consideramos que la Asamblea Legislativa debe contar con la debida claridad sobre las implicaciones jurídicas a nivel nacional e internacional que implica, la posible

aprobación de un instrumento internacional suscrito por Costa Rica, al comprometerse con obligaciones regidas por el Derecho Internacional y que gozarán de autoridad superior a las leyes.

En el caso que nos ocupa analizar, la Adhesión al Convenio sobre Ciberdelincuencia[42], y que a éste se han sumado una importante cantidad de miembros[43], por considerarse el estándar mundial en la ciberdelincuencia. Tema que es de particular interés regularlo en nuestro país, por los vacíos jurídicos en esta materia. Lo cual potencia el valor normativo de este Convenio Internacional, para acudir a esta fuente jurídica, y resolver éstos temas e integrarlo a las leyes y la Constitución Política para brindar una solución satisfactoria a esas omisiones.

De manera que a continuación, realizaremos una reseña de los temas que versa el Convenio sobre ciberdelincuencia. Este Convenio está conformado por cuatro capítulos.

El Capítulo Primero se refiere a la terminología, donde en su artículo 1 se establecen las definiciones de sistema informático, datos informáticos, proveedor de servicios y datos sobre le tráfico.

En el Capítulo Segundo se regulan las medidas legislativas que deberán adoptarse a nivel nacional cada Parte que se adhiera al presente Convenio. Este capítulo tiene una estructura de tres secciones, referentes a las medidas de derecho penal sustantivo, derecho procesal, y jurisdicción.

El **aspecto del derecho penal sustantivo** se subdivide en cinco títulos, donde se indica que **deben ser regulados en nuestro derecho interno, adoptando medidas legislativas y de otro tipo que resulten necesarias para tipificarse como delito penal, veamos:**

1. *Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos*
2. *Delitos informáticos*
3. *Delitos relacionados con el contenido* - pornografía infantil-
4. *Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines*
5. *Otras formas de responsabilidad y de sanciones*

Los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, regulan el acceso ilícito –art. 2-, interceptación ilícita –art.3-, interferencia en los datos –art. 4-, interferencia en el sistema –art. 5-, abuso de los dispositivos –art.6-.

---

[42] Para adherirse al Convenio sobre la Ciberdelincuencia, se debe contar con la invitación del Comité de Ministros del Consejo de Europa. Y en el caso de Costa Rica, se curso dicha invitación en la reunión sostenida a nivel de delegados el 31 de enero de 2007.

[43] Son Partes de este Convenio los siguientes miembros del Consejo de Europa: Albania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Estonia, Finlandia, Francia, Alemania, Hungría, Islandia, Italia, Letonia, Lituania, Malta, Moldavia, Montenegro, Reino de los Países Bajos, Noruega, Portugal, Rumania, Serbia, Eslovaquia, España, Eslovenia, Antigua República Yugoslava de Macedonia, Suiza, Ucrania y Reino Unido. Asimismo, como Parte de este Convenio, aparece los Estados Unidos de América, el cual no es miembro del Consejo de Europa.

En los delitos informáticos se regula la Falsificación informática –art. 7- y el fraude informático –art. 8-.

En los delitos relacionados con el contenido se regula los delitos **relacionados con la pornografía infantil –art. 9**[44]-. Este numeral **permite a cualquier Parte reservarse en todo o en parte el derecho de no aplicar las siguientes conducta**s:

- la **adquisición** de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
- la **posesión** de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

Y reservarse el concepto de «pornografía infantil», del material pornográfico que contenga la representación visual de:

- una persona que parezca un menor comportándose de una forma sexualmente explícita;
- imágenes realistas que representen un menor comportándose de una forma sexualmente explícita.

Con este tipo de reservas, **se permite a las Partes establecer diferencias en definiciones y conductas a sancionar, lo cual puede hacer inaplicable la disposición que regula esta materia. Por lo que se llama la atención en este sentido para efectos de las reservas del caso y tomando en consideración la sensibilidad del tema.**

En los delitos relacionados con infracciones de la **propiedad intelectual** y de los derechos afines se regula los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines –art. 10[45]-, **se remite a otras obligaciones**

---

[44] ***"Artículo 9. Delitos relacionados con la pornografía infantil***
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito penal en su derecho interno, la comisión deliberada e ilegítima de los siguientes actos:
a. la producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;
b. la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;
c. la difusión o transmisión de pornografía infantil por medio de un sistema informático;
d. la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;
e. la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.
2. A los efectos del anterior apartado 1, por «pornografía infantil» se entenderá todo material pornográfico que contenga la representación visual de:
a. un menor comportándose de una forma sexualmente explícita;
b. una persona que parezca un menor comportándose de una forma sexualmente explícita;
c. imágenes realistas que representen un menor comportándose de una forma sexualmente explícita.
3. A los efectos del anterior apartado 2, por «menor» se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.
4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2."

[45] ***"Artículo 10. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines***
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar

internacionales para que éstas sean tipificadas por infracción de la propiedad intelectual.

En las otras formas de responsabilidad y de sanciones, se regula **la tentativa y complicidad** –art 11-, **responsabilidad de las personas jurídicas** –art 12[46]-, sanciones y medidas–art 13[47]-. **La gran novedad en este título, es la responsabilidad a las personas jurídicas con su respectiva sanción.**

La opinión emitida por parte de la Procuraduría General de la República[48] en el expediente legislativo sobre la Adhesión al Convenio sobre la ciberdelincuencia, reitera

---

*como delito penal en su derecho interno, las infracciones de la propiedad intelectual, según se definen en la legislación de dicha Parte, de conformidad con las **obligaciones asumidas en aplicación del Acta de París del 24 de julio de 1971 por la que se revisó el Convenio de Berna para la protección de 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 Propiedad Intelectual**, a excepción de cualquier derecho moral otorgado por dichos convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.*

*2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para **tipificar como delito penal en su derecho interno**, las infracciones de los derechos afines definidos por la legislación de dicha Parte, de conformidad con **las obligaciones que ésta haya asumido por aplicación de la Convención Internacional sobre la Protección de los Artistas 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 las obras de los intérpretes y ejecutantes y los fonogramas**, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.*

*3. En circunstancias bien delimitadas, **cualquier Parte podrá reservarse el derecho a no exigir responsabilidad penal** en virtud de **los apartados 1 y 2** del presente artículo, siempre que **se disponga de otros recursos efectivos** y que **dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente artículo."*** (El destacado no es del original)

[46] ***"Artículo 12. Responsabilidad de las personas jurídicas***

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas, por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:

a. un poder de representación de la persona jurídica;

b. una autorización para tomar decisiones en nombre de la persona jurídica;

c. una autorización para ejercer funciones de control en la persona jurídica.

*2. Además de los casos ya previstos en el apartado 1 del presente artículo, **cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física** mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.*

*3. Con sujeción a los principios jurídicos de cada Parte, **la responsabilidad de la persona jurídica podrá ser penal, civil o administrativa**.*

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito." (El destacado no es del original)

[47] ***"Artículo 13. Sanciones y medidas***

*1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en los artículos 2 al 11 puedan dar lugar a la aplicación de **sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad**.*

*2. Cada Parte garantizará la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, **incluidas las sanciones pecuniarias, a las personas jurídicas consideradas responsables** de conformidad con el artículo 12."* (El destacado no es del original)

[48] **Procuraduría General de la República**, Oficio N° OJ de 31 de octubre de 2012, suscrito por José

lo manifestado a la Oficina Asesora de Tratados del Ministerio de Relaciones Exteriores, en su oficio OJ-057-2006 de 24 de abril de 2006, donde remite criterio técnico jurídico sobre la posible adhesión de Costa Rica al Convenio sobre la Ciberdelincuencia.

En dicha opinión[49] se describen las figuras jurídicas que se regulan en nuestro ordenamiento jurídico, y determinando la ausencia de otras figuras que deben ser implementadas para cumplir con las obligaciones del presente Convenio. A continuación se realiza una breve reseña de dichas figuras. Veamos:

> **Acceso ilícito** –art. 2 del Convenio- el Código de Normas y Procedimientos Tributarios –art. 94 acceso desautorizado a la información-, la Ley General de Aduanas –art. 221 delitos informáticos-, y el Código Penal -art. 196 bis violación de comunicaciones electrónicas-.
> **Interceptación ilícita** –art. 3 del Convenio- la totalidad de conceptos que abarca este numeral no se hayan recogidas íntegramente en la legislación costarricense. En el Código Penal –art. 96 bis violación de comunicaciones electrónicas, el 229 bis alteración de datos y sabotaje informático, párrafo primero-, en el Código de Normas y Procedimientos Tributarios –art. 95 manejo indebido del programas de cómputo- y la Ley General de Aduanas –art. 221 delitos informáticos-.
> **Abuso de los dipositivos** –art. 6 del Convenio- no existe en Costa Rica una disposición similar. Por lo que se hace necesaria la creación legislativa expresa y que su contenido tenga alcances generales. El delito denominado **"suplantación de personalidad"** tampoco se encuentra regulado en la legislación nacional, solo se pena la conducta en materia tributaria y aduanera. En el Código de Normas y Procedimientos Tributarios –art. 96 facilitación del código y la clave de acceso y art. 97 préstamo de código y clave de acceso-, y la Ley General de Aduanas introduce un tipo de responsabilidad objetiva –art. 105 código y clave de acceso y prueba de los actos realizados en sistemas informáticos. La Ley General de Aduanas castiga la entrega a terceros no autorizados del nombre de usuario y palabras de acceso, incluyendo si el hecho ocurre de manera culposa –art. 221 delitos informáticos y 222 agravante-, y la Ley de Administración Financiera de la República y Presupuestos Públicos castiga la entrega a personas no autorizadas del código y clave de acceso, aunque no si el hecho se llevase a cabo de manera culposa –art. 111-.
> **Falsificación informática** –art. 7 del Convenio- el Código Penal sanciona la alteración de datos y el sabotaje informático, el acceso, borrado, supresión, modificación o inutilización no autorizada de datos registrados en una computadora, se da mayor pena si el actuar ilícito se entorpece o inutiliza un programa de cómputo base de datos o sistema informático, y se eleva la pena si si el ataque es cometido contra sistemas de información de naturaleza pública –art. 229 bis-.
> **Fraude informático** –art. 8 del Convenio- el Código Penal –art. 217 bis-
> **Delitos relacionados con la pornografía infantil** –art. 9 del Convenio- Costa Rica ha procurado mantener una actitud de salvaguarda de los derechos de los menores, protegiendo precisamente la indemnidad e inexperiencia sexual de los potenciales afectados. Con el Protocolo Facultativo de la Convención sobre los

---

Enrique Castro Marín, Procurador Director.
[49] Ibid.

Derechos del Niño relativo a la venta de niños, la prostitución infantil y utilización de niños en la pornografía y el Código Penal –art. 174-.

Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines –art. 10 del Convenio- se encuentran reguladas en la Ley de Derechos de Autor y Derechos Conexos y la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual.

Responsabilidad de las personas jurídicas –art. 12 del Convenio- no existe legislación en nuestro país.

Conservación rápida de datos informáticos almacenados –art. 16 del Convenio- tampoco se tiene legislación expresa, en materia procesal penal, que trate expresamente de la conservación de datos informáticos.

De manera que se recomienda el análisis profundo de dicha opinión, así como las de de expertos en el tema que la Comisión pueda llamar en audiencia, para efectos de tener claras las posibles modificaciones que deben ser abordadas en las diferentes leyes que regulan las conductas de los delitos informáticos. Y solventar las muchísimas carencias y normas incompletas, con el objeto de armonizarlas con las conductas descritas en el Convenio en estudio, para una adecuada implementación del mismo.

En el **aspecto del derecho procesal del Convenio**, se subdivide en cinco títulos, donde se indica la necesidad de regular en nuestro derecho interno, las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos para fines de investigaciones o procedimientos penales específicos, veamos:

1. Disposiciones comunes
2. Conservación rápida de datos informáticos almacenados
3. Orden de presentación
4. Registro y confiscación de datos informáticos almacenados
5. Obtención en tiempo real de datos informáticos

En las disposiciones comunes se regula el ámbito de **aplicación de las disposiciones sobre procedimiento** –art. 14[50]-, y las condiciones y salvaguardas -art. 15-. Estos

---

[50] ***"Artículo 14. Ámbito de aplicación de las disposiciones sobre procedimiento***

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente sección para los fines de investigaciones o procedimientos penales específicos.

2. Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:

a. los delitos penales previstos de conformidad con los artículos 2 a 11 del presente Convenio;

b. otros delitos cometidos por medio de un sistema informático; y

c. la obtención de pruebas electrónicas de un delito.

3. a. Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.

b. Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:

i. *utilizado en beneficio de un grupo restringido de usuarios, y no utilice las redes públicas de comunicaciones ni esté conectado a otro sistema informático, ya sea público o privado, dicha Parte*

numerales son de suma importancia, puesto que los poderes y procedimientos para los fines de investigaciones o procedimientos penales específicos se aplicarán sujetos a estas disposiciones -artículos 16, 17, 18, 19, 20 y 21 del Convenio de Adhesión-. Se establecen excepciones a estas aplicaciones de poderes y procedimientos ver artículo 21[51] del Convenio.

En la conservación rápida de datos informáticos almacenados se regula la conservación rápida de datos informáticos almacenados –art. 16- y la conservación y revelación parcial rápidas de datos sobre el tráfico –art. 17-. En cuanto a la conservación rápida de datos informáticos almacenados se regula la conservación rápida de datos informáticos almacenados, se establece el compromiso de obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a **mantener en secreto** la aplicación de dichos procedimientos durante el plazo previsto por su derecho interno, esto quiere decir que se debe tomar medidas legislativas para regular en este sentido.

En la regulación de orden de presentación -artículo 18[52] se faculta a las autoridades que se designen competentes –en Costa Rica- para ordenar a **una persona** que se

---

podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21."

[51] ***"Artículo 21. Interceptación de datos sobre el contenido***

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:

a. a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica

i. a obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o

ii. a prestar a las autoridades competentes su asistencia y su asistencia para obtener o grabar, en tiempo real, los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.

2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquier de los poderes previstos en el presente artículo, así como toda información al respecto

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15."

Además, se posibilita las reservas a aplicar en los siguientes supuestos de obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio. O el delito de obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica: obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o a prestar a las autoridades competentes su asistencia y su asistencia para obtener o grabar, en tiempo real, los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático (regulado en el numeral 20 del Convenio). Sin embargo, se indica de seguido que las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20."

[52] ***"Artículo 18. Orden de presentación*** *Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:*

a. a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y

b. a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte, que

encuentre en el territorio nacional que **comunique determinados datos informáticos que posea** o que **se encuentren bajo su control**, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y al **proveedor de servicios** que ofrezca prestaciones en el territorio nacional, para que **comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios**.

Para ello, se define como **«datos relativos a los abonados»** a toda información, en forma **de datos informáticos o de cualquier otra forma**, que **posea un proveedor de servicios** y **esté relacionada con los abonados a dichos servicios**, para determinar:

a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;
b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;
c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

De forma que con el afán de garantizar el derecho a la intimidad, a la libertad y al secreto de las comunicaciones, resguardado en nuestra Constitución Política -artículo 24-, se considera esencial cumplir con la mayoría calificada en caso de querer autorizar dicho acceso a los datos antes descritos.

En lo relativo al registro y confiscación de datos informáticos almacenados –art. 19- se realiza la misma observación del artículo 24 constitucional. En razón que se establece una serie de facultades a las autoridades competentes para registrar o a tener acceso a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos. Así como proceder al registro y acceso de una forma similar a un sistema informático específico o a una parte del mismo. El confiscar para obtener los datos informáticos a los que se haya tenido acceso, así como realizar y conservar una copia de dichos datos informáticos; c. preservar la integridad de los datos informáticos almacenados de que se trate; hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso. Y por último ordenar a cualquier persona que conozca el funcionamiento del sistema

---

comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.
Los poderes y procedimientos mencionados en el presente artículo están sujetos a lo dispuesto en los artículos 14 y 14.
A los efectos del presente artículo, por «datos relativos a los abonados» se entenderá toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:
a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;
b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;
c. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios."

informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria.

En la obtención en tiempo real de datos informáticos, el cual regula la obtención en tiempo real de datos de tráfico –art. 20[53]- y la interceptación de datos sobre el contenido –art. 21[54]-, aplica las mismas observaciones anteriores del numeral 24 constitucional.
A manera de reflexión para esta sección de derecho procesal, el Instituto Costarricense de Electricidad[55], señaló la necesidad de creación de normas procesales que estén enfocadas a la acreditación del tipo de delitos regulados en este Convenio, y con ello dotar de capacitación y herramientas tecnológicas, a quienes serán los responsables de llevar a cabo este tipo de investigaciones, lo cual consecuentemente provocará la necesidad de realizar una inversión económica importante en el país.

---

[53] ***Artículo 20. Obtención en tiempo real de datos de tráfico***
1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a:
a. obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y
b. obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:
i. obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o
ii. a prestar a las autoridades competentes su asistencia y su asistencia para obtener o grabar, en tiempo real, los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1 .a), podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poder artículo, así como toda información al respecto.
4. *Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15."*

[54] ***"Artículo 21. Interceptación de datos sobre el contenido***
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:
a. a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio; y
b. obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica
i. a obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o
ii. a prestar a las autoridades competentes su asistencia y su asistencia para obtener o grabar, en tiempo real, los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.
2. Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.
3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquier de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15."

[55] **Instituto Costarricense de Electricidad.** Oficio N° 256-168-2012 del 27 de setiembre de 2012, suscrito por Julieta Bejarano Hernández, Jefe División Jurídica.

Además, esta institución coincide con nuestro criterio sobre la valoración que debe realizarse por parte del Estado costarricense, por los compromisos adquiridos a nivel internacional con la adhesión a éste Convenio, relacionado con los principios y obligaciones desarrollados en éste. El ICE[56] hace especial referencia a la creación del procedimiento de asistencia mutua, así como los temas de interceptación de datos sobre el contenido de determinadas comunicaciones transmitidas en territorio costarricense, y en la conservación y revelación rápida de datos conservados sobre el tráfico y datos informativos almacenados en los sistemas de los proveedores de servicios.

Incluso, se hace la observación[57] acerca de la **exigencia para los operadores de redes y proveedores de acceso (ICE**), asociadas a brindar colaboración a las autoridades competentes, para la obtención en tiempo real de datos de tráfico o datos sobre el contenido asociados a determinadas comunicaciones transmitidas en su territorio, lo cual evidentemente **generaría la obligación de realizar grandes inversiones económicas**, no obstante, al indicarse que estas obligaciones se encuentran condicionadas a la capacidad técnica del obligado en ese momento, **las mismas adquieren flexibilidad y resultan manejables para el ICE y los demás operadores y proveedores de servicios de telecomunicaciones**, toda vez que éstos ya se encuentra obligados en virtud de la Ley contra la Delincuencia Organizada a brindar la colaboración necesaria para la oportuna y eficaz operación del Centro Judicial de Intervenciones de las Comunicaciones (CJIC). Por lo que se deja patente el comentario para una reflexión e implementación en las normas del presente Convenio.

El **aspecto jurisdiccional** que establece el Convenio –art. 22- indica que los delitos previstos en los artículos del 2 al 11 del Convenio podrán ser de nuestra jurisdicción siempre que se hayan tomado las medidas legislativas y que se haya cometido: en el territorio nacional; a bordo de un buque que enarbole pabellón de Costa Rica; a bordo de una aeronave matriculada según las leyes de Costa Rica; por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en que se cometió o si ningún Estado tiene jurisdicción territorial respecto del mismo.
En el punto 2 de este artículo se establece la facultad del Estado de reservarse el derecho a no aplicar, o a aplicar únicamente en determinados casos o condiciones, las normas sobre jurisdicción establecidas en cuanto a delitos cometidos a bordo de un buque que enarbole pabellón de dicha Parte, o por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en que se cometió o si ningún Estado tiene jurisdicción territorial respecto del mismo. Incluso se señala que la reserva aplica “en cualquiera otra parte de los mismos”, entiéndase de las circunstancias descritas en el párrafo anterior.

En el punto 3 del artículo se indica que el Estado adoptará las medidas necesarias para atribuirse la jurisdicción de los delitos que se señalan en el artículo 24 sobre extradición, apartado 1[58], cuando el presunto autor del delito se encuentre en su

---

[56] Ibid.
[57] Ibid.
[58] *“Los delitos establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave. Y cuando deba aplicarse una pena mínima diferente, en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24),*

territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

En el punto 5 se establece que cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales. En este aspecto es conveniente determinar quién será la autoridad competente encargada para esos efectos, lo cual se puede desarrollar en las normas de implementación de este Convenio.

En el Capítulo Tercero se regula la **cooperación internacional**. Este capítulo tiene una estructura de dos secciones, referentes a principios generales y disposiciones especiales.

El **aspecto de los principios generales** se subdivide en cuatro títulos, donde se establecen:

1- Principios generales relativos a la cooperación internacional
2. Principios relativos a la extradición
3- Principios generales relativos a la asistencia mutua
4.- Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Los Principios generales relativos a la cooperación internacional -art. 23-, establece la cooperación de las Partes "en la mayor medida posible", en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigación o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

En los principios relativos a la extradición –art. 24- se aplicará la extradición entre las Partes los delitos establecidos en los artículos 2 a 11 del presente Convenio. En el punto 5 se indica que la extradición estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición. Y el punto 6 [59] se establece la condición por la cual puede denegarse la extradición. Se indica que el trámite de la extradición se realizará ante *"sus autoridades competentes"*, por lo que es de especial interés indicar en la ley de implementación cuál será esas *"autoridades competentes"* para el caso de Costa Rica. Pues como se indica en el

---

se aplicará la pena mínima establecida en virtud de dicho acuerdo o tratado."

[59] *Artículo 24 …*

6. Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo, únicamente ***por razón de la nacionalidad de la persona buscada*** *o porque* ***la Parte requerida se considera competente respecto de dicho delito****, la Parte requerida deberá someter el asunto –a petición de la Parte requirente—a sus autoridades competentes para los fines de las actuaciones penales pertinentes e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable de conformidad con la legislación de dicha Parte. (El destacado no es del original).*

punto "7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, ***el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado****.*
b. El Secretario General del Consejo de Europa ***creará y mantendrá actualizado un registro de las autoridades designadas por las Partes****. Cada Parte* ***garantizará la exactitud de los datos que figuren en el registro."*** *(El destacado no es del original).*

En cuanto a los **principios generales relativos a la asistencia mutua** –art. 25- es para fines de investigaciones y procedimientos relativos a delitos relacionados a sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito. Para ello se establece necesario tomar medidas legislativas para cumplir las obligaciones de los artículos del 27 al 35[60]. En el punto 3 se establecen medios de comunicación en caso de emergencia. En el punto 4 indica que la Parte no podrá ejercer el derecho a denegación de asistencia mutua sobre los delitos del 2 al 11[61], únicamente porque la solicitud se refiere a un delito que considere de naturaleza fiscal. En el punto 5 se hace referencia a la doble tipificación penal siempre que esté constituida en el derecho interno, por lo que se deja constando para su debida implementación.

En la **información espontánea** -art. 26- relativo a comunicar información obtenida en investigaciones, cuando la información podrá ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos. En punto 2 se establece que la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. No obstante, de seguido se indica que *"si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello, debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas"*. Por lo que este tipo de información espontánea debe valorarse a la luz de nuestro derecho interno, ya que eventualmente podría acarrear responsabilidades al Estado.

En los **procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables** –art. 27- en el punto 1 a. se hace referencia a la designación de la o las autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a

---

[60] **Artículo 27**.- Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables, **artículo 28** - Confidencialidad y restricción de la utilización
Artículo 29 - Conservación rápida de datos informáticos almacenados, **artículo 30** - Revelación rápida de datos conservados sobre el tráfico, **artículo 31** - Asistencia mutua en relación con el acceso a datos informáticos almacenados, **artículo 32** - Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público, **artículo 33** - Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico, **artículo 34** - Asistencia mutua relativa a la interceptación de datos sobre el contenido y **artículo 35** - Red 24/7.

[61] **Artículo 2**. Acceso ilícito, **artículo 3.** Interceptación ilícita, **artículo 4**. Interferencia en los datos, **artículo 5.** Interferencia en el sistema, **artículo 6**. Abuso de los dispositivos, **artículo 7**. Falsificación informática, **artículo 8**. Fraude informático, **artículo 9.** Delitos relacionados con la pornografía infantil, **artículo 10**. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines y **artículo 11.** Tentativa y complicidad

las autoridades competentes para su ejecución. Las cuales deben ser indicadas en la legislación que se implemente para el Convenio. En el punto 8 se establece el mecanismo para la confidencialidad que tiene estrecha relación con la sugerencia apuntada en el artículo 26 del Convenio. En el punto 9 se establece que en caso de urgencia se acudirá directamente a las autoridades judiciales de la Parte, que cualquier solicitud o comunicación podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL). Sin embargo, se indica que *"en el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central*", por lo que se deja sentada esta posibilidad por si se desea hacer la solicitud del caso.

La **confidencialidad y restricción de la utilización** –art. 28 – se podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que: se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud. En todo caso, cualquier Parte que facilite información o material podrá requerir a la otra Parte que explique el uso dado a dicha información o material.

Las **disposiciones especiales** se subdivide en tres títulos, donde se establecen:

1- Asistencia mutua en materia de medidas provisionales
2.- Asistencia mutua en relación con los poderes de investigación
3- Red 24/7

En lo referente a la asistencia mutua en materia de medidas provisionales se regula la **conservación rápida de datos informáticos almacenados** –art. 29 – cada Parte podrá solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos. En el punto 2 se establece los indicadores de la solicitud. En el punto 3 indica que la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. En este aspecto se deja constando para efectos de tomar en cuenta para las normas de implementación del Convenio. En el punto 4 se establece el derecho a denegar la solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, cuando una Parte exija la doble tipificación penal, la Parte podrá reservarse -en relación con delitos de los artículos 2 a 11 del presente Convenio-, por creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

En cuanto a la **revelación rápida de datos conservados sobre el tráfico** –art. 30 – indica la obligación para la Parte requerida cuando descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió

la comunicación. En el punto 2 establece la posibilidad de negativa de la revelación cuando se refiera a delitos políticos o relacionados con éstos, o que la solicitud atente contra la soberanía, seguridad, orden público u otros intereses esenciales de la Parte requerida.

En la temática de **asistencia mutua en relación con los poderes de investigación,** se regula **la asistencia mutua en relación con el acceso a datos informáticos almacenados** –art. 31-, el acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público –art. 32 – donde se señala que una Parte podrá, sin la autorización de la otra Parte, en punto a) a tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos y en punto b) si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático. En cuanto a **la asistencia mutua para la obtención en tiempo real de datos sobre el tráfico** –art. 33 - sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Para ello se deben establecer las condiciones y procedimientos mediante el derecho interno, de acuerdo con el punto 1 de este numeral. Por lo que se deja patente dicha observación, para efectos de las normas de implementación que deben desarrollarse para la aplicación del Convenio. En relación con **la asistencia mutua relativa a la interceptación de datos sobre el contenido** –art. 34 - las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático. Se establece la salvedad que siempre que lo permitan sus tratados y el derecho interno aplicables. Por lo que se deja constando esta situación para efectos de valoración sobre las normas de implementación que se deban promulgar.

En la **Red 24/7** –art. 35 – se indica que cada Parte designará un punto de contacto disponible las veinticuatro horas del día, siete días a la semana, que garantice la prestación de ayuda inmediata para las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. La asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas de el asesoramiento técnico; la conservación de datos -artículos 29 y 30-; y la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos

Este punto de contacto debe determinarse en las normas de implementación, para efectos de seguridad jurídica y de aplicación adecuada de esta obligación internacional. Incluso en el punto 2 b) del artículo 35 se indica que si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente. Estableciéndole una serie de funciones sumamente delicadas, por lo que debe especificarse quién será en Costa Rica el punto de contacto.

Además, en el punto 3 se indica que **cada Parte garantizará** la disponibilidad de **personal** debidamente **formado y equipado,** con objeto de facilitar el funcionamiento de la red. Por lo que se debe tener certeza de quienes serán los encargados de dicha

función, lo cual implicará una presupuestación para las obligaciones que se adquieren a nivel internacional.

En el Capítulo Cuarto se regulan las **disposiciones finales**. Este último capítulo se compone de trece artículos.

Lo referente a la firma y entrada en vigor del Convenio, -art. 36-, la adhesión al Convenio –art. 37[62] –, la aplicación territorial –art. 38 -, los efectos del Convenio –art. 39[63] -, lo relativo a las declaraciones –art. 40 –, sobre la cláusula federal -art. 41 -, lo referente a las reservas -art. 42[64]-, situación de las reservas y retirada de las mismas –art. 43 -, las enmiendas –art. 44 –, las solución de controversias -art. 45[65] -, consultas entre las Partes –art. 46[66] -, denuncia –art. 47 – y notificación –art. 48 –.
Con la referencia realizada de todas las disposiciones del Convenio sobre la ciberdelincuencia, podemos concluir que es un instrumento jurídico útil y eficaz para prevenir actos dirigidos contra la confidencialidad, integridad, disponibilidad y abuso de las nuevas tecnologías; proporcionando un marco mundial para aplicar una política

---

[62] Vigencia para Costa Rica, en el punto *"2.Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrar· en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa."*

[63] *"**Artículo 39 - Efectos del Convenio***

1. La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:

- el Convenio europeo de extradición, abierto a la firma en París el 13 de diciembre de 1957 (STE nº 24);

- el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE nº 30);

- el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE nº 99).

2. Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio.

3. Nada de lo dispuesto en el presente Convenio afectar· a otros derechos, restricciones, obligaciones y responsabilidades de las Partes."

[64] Solo las previstas en el apartado 2 del artículo 4, apartado 3 del artículo 6, apartado 4 del artículo 9, apartado 3 del artículo 10, apartado 3 del artículo 11, apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas.

[65] En el punto *"2. En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas."*

[66] Las consultas periódicas, versa sobre:

a. la utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;

b. el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico;

c. el estudio de la conveniencia de ampliar o enmendar el presente Convenio.

En el punto 4 se establece la salvedad en los casos en que sean asumidos por el Consejo de Europa, **los gastos** realizados para aplicar las consultas periódicas **serán sufragados por las Partes en la forma que éstas determinen**. Por lo que se deja constancia de esta situación para las previsiones presupuestarias del caso.

penal común destinada a proteger a la sociedad contra ciberdelincuencia. Buscando la cooperación internacional, en defensa de los derechos patrimoniales y derechos humanos fundamentales, la protección de menores, el derecho a la confidencialidad, el derecho a la intimidad, el derecho a la protección de las bases de datos personales.

Por lo que resulta de especial interés que el Estado costarricense procure la aprobación de la Adhesión al este Convenio, que involucran disposiciones en la aplicación de herramientas tecnológicas, urgentes de legislar en nuestro país.

Como se ha manifestado a lo largo de este informe jurídico, lo cual coincide con lo externado por la Procuraduría General de la República[67] en la opinión emitida sobre este proyecto de ley, en cuanto a "las comunicaciones es el campo donde el desarrollo tecnológico ha tenido su mayor expresión, y ello se evidencia en las múltiples opciones con que cuenta el ciudadano para realizar sus contactos, la velocidad, prontitud y seguridad con que puede ejecutarlas, y la constancia de los sistemas remotos, en tanto servicios públicos."

Por lo que el elemento esencial para combatir la ciberdelincuencia de forma efectiva, es la educación del usuario, para asegurar la protección de los usuarios y su información; así como la voluntad política para emitir una legislación equilibrada en lo técnico y lo jurídico.

En el aspecto de producción de la ley, hemos demostrado las limitaciones normativas existentes en nuestro país sobre el tema de delitos informáticos. Así como la necesidad de crear nuevas figuras que respondan a las necesidades sociales, producidas por la incorporación de las nuevas tecnologías de información y comunicación en nuestro medio.

Además, el carácter transnacional de los delitos informáticos, exige la adopción de medidas preventivas y represivas exitosas a nivel mundial, y es con la Adhesión a este Convenio, que se estaría encausando a este fin. No sin antes reiterar que por la naturaleza jurídica del convenio internacional -rango superior al de las normas comunes-, debe el legislador y la legisladora obligarse a armonizar la normativa de derecho interno, a fin de compatibilizarla plenamente con las disposiciones del Convenio sobre ciberdelincuencia. Y de esta manera se protegerá a los usuarios y la información de la ciberdelincuencia, mejorando la cooperación internacional en esta materia.

Finalmente, como un dato adicional esta asesoría se permite recordar a las señoras y señores diputados la existencia de la reciente "Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales", Nº 8968 de de 7 de julio de 2011, en virtud de que precisamente tutela información relacionada con el derecho a la intimidad, y que frecuentemente resulta ser violentada mediante el uso de medios informáticos. Mediante este instrumento jurídico se reconoce en forma expresa el derecho fundamental de toda persona física o jurídica a conocer la información que conste sobre ella, sus bienes o derechos en cualquier registro o archivo, de toda naturaleza y sanciona el manejo ilegal de dicha información.

[67] Op. Cit. Procuraduría General de la República.

En el artículo 1 de la ley de cita se establece expresamente el objetivo en los siguientes términos:

> **"ARTÍCULO 1.- Objetivo y fin**
> Esta ley es de orden público y tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes."

Por su parte el artículo 2 indica el ámbito de aplicación y establece:

> **"ARTÍCULO 2.- Ámbito de aplicación**
> Esta ley será de aplicación a los datos personales que figuren en bases de datos automatizadas o manuales, de organismos públicos o privados, y a toda modalidad de uso posterior de estos datos.
>
> El régimen de protección de los datos de carácter personal que se establece en esta ley no será de aplicación a las bases de datos mantenidas por personas físicas o jurídicas con fines exclusivamente internos, personales o domésticos, siempre y cuando estas no sean vendidas o de cualquier otra manera comercializadas."

Los contenidos de esta normativa encuentran relación con parte de los alcances del Convenio y los compromisos que se estarían adoptado, considerando que la autodeterminación informativa es una ampliación del derecho a la intimidad y que su protección surge a partir del desarrollo de mecanismos informáticos y tecnológicos globales que manejan bases de datos que contienen información de las personas.

IV.- ASPECTOS DE TÉCNICA LEGISLATIVA

Para efectos de una adecuada técnica legislativa, se debe armonizar lo indicado en el título del proyecto de ley, en la exposición de motivos y el articulado, para que exista una concordancia en lo que se pretende someter a consideración del Poder Legislativo.

De manera que se observa, desde el inicio del expediente (ver folio 1), en el oficio LYD 5248-C de fecha 10 de mayo de 2012, que remite el Ministerio de la Presidencia a la Secretaria de la Asamblea Legislativa, que el proyecto de ley plantea una aprobación de Adhesión al Convenio, indicando que *"se presenta para el conocimiento de la Asamblea Legislativa el proyecto de Ley* ***"Aprobación de la Adhesión al Convenio sobre ciberdelincuencia"****, con el propósito de que como iniciativa del Poder Ejecutivo, se le dé el trámite de rigor."*

En la exposición de motivos se señala que es una **Adhesión** al Convenio, así como en el título de la iniciativa. Sin embargo, en el enunciado del artículo único del proyecto se omite que es una Adhesión al Convenio. Por lo que se llama la atención en ese sentido, para que en el contenido del Artículo Único del proyecto de ley, se consigne en forma expresa la frase "Aprobación de la Adhesión al" antes de la oración "Convenio sobre ciberdelincuencia".

Es relevante indicar que en el folio N° 12 Expediente físico, consignado como folio 10 en el texto digital registrado en el SIL; del instrumento que se pretende aprobar, se consigna al inicio de esas páginas el siguiente párrafo "**YO, KATIA MARÍA JIMÉNEZ**

POCHET, TRADUCTORA OFICIAL DEL MINISTERIO DE RELACIONES EXTERIORES Y CULTO DE LA REPUBLICA DE COSTA RICA, NOMBRADA POR ACUERDO NUMERO 8-DJ DEL 21 DE NOVIEMBRE DEL 2000 PUBLICADO EN LA GACETA NUMERO 45 DEL 5 DE MARZO DE 2001, CERTIFICO QUE LA TRADUCCIÓN DEL IDIOMA INGLÉS AL IDIOMA ESPAÑOL DEL SIGUIENTE DOCUMENTO DICE LO SIGUIENTE:". Así como el párrafo del folio N° 44 Expediente físico, consignado como folio 41 en el texto digital registrado en el SIL, que indica "**EN FE DE LO CUAL SE EXPIDE LA PRESENTE TRADUCCIÓN OFICIAL DEL INGLÉS AL ESPAÑOL COMPRENSIVA DE TREINTA Y TRES FOLIOS. FIRMO Y SELLO EN LA CIUDAD DE SAN JOSÉ, COSTA RICA AL DÍA DIECINUEVE DE ABRIL DE DOS MIL DOCE. SE ADJUNTAN Y CANCELAN LOS TIMBRES DE LEY Y SE ANULA EL REVERSO DE CADA FOLIO", lo cual constituyen materia ajena** del contenido del Artículo Único, por consiguiente, ***se sugiere suprimir por medio de moción de forma lo establecido en dichos folios.*** Esto significa que el texto del instrumento internacional que se pretende aprobar, comienza a partir de "CONVENIO SOBRE CIBERDELINCUENCIA" y finalizar en *"Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitir copias certificadas a cada uno de los Estados Miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado invitado a adherirse al mismo."*

Igualmente, es necesario **trasladar al final del expediente moción de forma** el contenido del folio N° 45 del expediente físico, consignado como folio 42 en el texto digital registrado en el SIL, por cuanto este último folio contiene una Certificación emitida por Estela Blanco Solís, Directora General a.i. de Política Exterior, documento que **no forma parte del instrumento internacional sometido a conocimiento de la** Asamblea Legislativa y solamente funge como elemento de constatación.

Al respecto cabe anotar, que este Departamento, se pronunció con ocasión de una consulta en un caso de similar naturaleza al que se estudia, mediante oficio CON-043-2012, y se indicó:

> *"Cabe señalar que la Constitución Política en el artículo 121 inciso 4) confiere al Poder Legislativo la competencia para "aprobar o improbar los convenios internacionales, tratados públicos y concordatos…", por lo que queda claro que la Asamblea Legislativa al tramitar este tipo de instrumentos internacionales solo puede aprobarlos o improbarlos, de tal manera que el legislador no puede realizar modificaciones por ser un acuerdo de voluntades entre sujetos de derecho internacional.*
>
> *Sin embargo, las frases objeto de esta consulta, no forman parte del convenio o acuerdo de voluntades entre sujetos de derecho internacional, simplemente se trata de un "addendum" incorporado por el Poder Ejecutivo donde se certifica que se cumple con las formalidades requeridas para dar curso al trámite legislativo.*
>
> ***Por tratarse de aspectos forma, que no constituyen parte del instrumento internacional, dichos certificados o extremos que responden a requisitos para poder realizar la negociación, y que deben formar parte del expediente no del convenio, deben ser eliminados del texto, mediante una moción de forma[68], preferentemente por la Comisión Dictaminadora."***

[68] *Sobre este particular ver el artículo 152 del Reglamento de la Asamblea Legislativa.*

Asimismo, este Departamento mediante oficio N° CON-26-2012-J señaló[69]: *"en aquellos casos en que los proyectos sobre tratados o convenios internacionales estén siendo analizados por la* ***Comisión Permanente de Redacción, dicha Comisión puede proceder a la eliminación de los certificados o información que no forme parte de las cláusulas del convenio internacional****, negociado por el Poder Ejecutivo, en virtud de las atribuciones y potestades que el Reglamento Legislativo otorga a la Comisión Permanente Especial de Redacción en los artículos 85 inciso c) 141, 142, 152 y 159."*

La Sala Constitucional, en el Voto N° 7004-94 de las nueve horas dieciocho minutos del dos de diciembre de mil novecientos noventa y cuatro, con respecto a inclusiones de textos en artículos de los Convenios, que son ajenas a la materia propia de éstos y por consiguiente no deben ser aprobados por la Asamblea Legislativa, ha sostenido:

> *"La Asamblea Legislativa deberá con absoluta claridad, especificar que los instrumentos suscritos por Costa Rica con la intención de obligarse, regidos por el Derecho Internacional y que gozarán de "autoridad superior a las leyes", son los indicados por el Poder Ejecutivo y respecto de los cuales es necesario cumplir los trámites legislativos de aprobación. Sobre todo porque el "Artículo 1° del Proyecto de Ley dice: Se aprueba el Acta final en que se incorporan los Resultados de la Ronda de Uruguay de Negociaciones Comerciales Multilaterales", incluyendo los siguientes acuerdos y declaraciones ministeriales" (…).* ***En consecuencia, las Declaraciones y Decisiones Ministeriales y los Acuerdos Plurinacionales no constituyen un tratado o convenio internacional y por ende no deben ser aprobados por la Asamblea Legislativa y deben ser excluidos del todo de la ley de aprobación del tratado y convenios internacionales citados****. (…) Hecha la distinción entre el contenido del Acta Final de carácter normativo vinculante para nuestra Nación, y el contenido que no goza de esa condición jurídica según se ha expuesto y en tanto se produzca la separación completa de las normas vinculantes de las otras, esta Sala emite su opinión favorable al Convenio tanto en los aspectos de procedimientos constitucionales necesarios para perfeccionar la obligación internacional contraída por nuestra Nación."*[70] (El resaltado no es de original).

En el artículo 18 punto 3. del Convenio en estudio, se hace una remisión a *"los artículos* ***14 y 14****",* por considerarse que es un **error material, se recomienda de considerarse necesario una breve consulta a la Cancillería para que ésta revise el texto original del Convenio para determinar la remisión adecuada**. Y así poder consignar adecuadamente, mediante las notas respectivas, la remisión correcta al artículo. **De toda suerte, esta asesoría considera por la lectura integral del Convenio en estudio, que se puede comprender que la remisión se pretende a los artículos 14 y 15 referidos a las regulaciones de los poderes, procedimientos de investigaciones o procedimientos penales específicos.**

La misma observación aplica para el artículo 19 del Convenio, al establecerse en el numeral cinco puntos a regular; sin embargo por un error material, se consignan dos puntos dos, en lugar de ser dos y tres. Por lo que se deja planteada dicha situación

---

[69] *CON-026-2012 j., de 20 de marzo de 2012 elaborada por la Licda. Tatiana Arias Ramírez y la Licenciada Rebeca Quesada, Asesoras Parlamentarias y revisada por la Licda. Gloria Valerín Rodríguez.*

[70] Voto de la Sala Constitucional N° 7004-94, de las nueve horas dieciocho minutos del dos de diciembre de mil novecientos noventa y cuatro.

para que se aplique el mismo procedimiento de corrección mediante las notas correspondientes de Cancillería, para realizar la modificación material.

En cuanto al artículo 20 punto b subinciso ii, se repite la frase "su asistencia", y en el punto 3 del Convenio se indica la siguiente oración "de los poder artículo", la cual no se comprende claramente. Y en el artículo 21 punto 3 se consigna una cláusula similar que indica la frase de la siguiente manera "de los poderes previstos en el presente artículo", la cual hace que cobre sentido el argumento. Por lo que se dejan constancia de los errores materiales para que éstos pueda ser subsanado como anteriormente se indicó, mediante las notas correspondientes de Cancillería, para realizar la modificación material.

En igual sentido se consigna error material en la conjugación de un verbo, lo cual puede obedecer a la traducción del Convenio, específicamente en el artículo 30 punto 1. en la frase que dice "la Parte requerida revelar rápidamente a la Parte requirente" lo que se entiende que debe decir es "la Parte requerida revelará rápidamente a la Parte requirente". Por lo que se dejan constancia del error material para que éste pueda ser subsanado como anteriormente se indicó, mediante las notas correspondientes de Cancillería, para realizar la modificación material.

V.- ASPECTOS DE PROCEDIMIENTO LEGISLATIVO

A. Verificación de los plenos poderes en el instrumento internacional[71]

Para efectos de los plenos poderes en la **Adhesión** a un Convenio Internacional, recordemos lo indicado en el apartado "Sobre la adhesión a un Convenio Internacional" de este informe jurídico, al manifestar la Sala Constitucional[72] que:

> *"en atención a lo dispuesto en los artículos 2 y 11 de la Convención de Viena sobre el Derecho de los Tratados (Ley Nº 7615 de 24 de julio de 1996,* ***la adhesión es el acto internacional por el cual un Estado hace constar en el ámbito internacional su consentimiento en obligarse por un tratado que no fue negociado directamente por éste****.* ***Y el artículo 15*** *de la Convención de Viena sobre el Derecho de los Tratados establece, en su inciso a), que* ***el consentimiento de un Estado en obligarse por un tratado se manifiesta mediante la adhesión cuando el propio tratado disponga tal posibilidad.*** *…"* (El resaltado no es del original).

Sobre esta misma materia, agregó esta jurisprudencia constitucional que:

> *"en el caso del citado artículo 11 de la Convención de Viena sobre el Derecho de los Tratados, el Gobierno de Costa Rica hizo la reserva en el sentido de que el sistema jurídico constitucional de nuestro país no autoriza ninguna forma de consentimiento que no esté sujeto a la ratificación de la Asamblea Legislativa. Ello en atención a lo dispuesto en el inciso 4), del artículo 121 de la Constitución Política, que establece que corresponde, exclusivamente, a la Asamblea Legislativa aprobar o improbar los convenios internacionales, tratados públicos y concordatos.* ***Este Tribunal ya se ha***

---

[71] Tomado del Informe del **Departamento de Servicios Técnicos**, Oficio ST N° 158-2012 J de 9 de agosto del 2012, sobre el expediente Nº 18.382, proyecto de ley: "Aprobación de la Adhesión a la Convención para facilitar el acceso internacional a la justicia".

[72] **Sala Constitucional**. Voto N° 18209-2008 de las 18:17 horas del 10 de diciembre del 2008.

pronunciado sobre el procedimiento de adhesión a un instrumento internacional, y ha manifestado que ésta no infringe el Derecho de la Constitución, siempre que conste la voluntad del Poder Ejecutivo de obligarse por dicho instrumento, y que este sea sometido a aprobación del órgano parlamentario." (El resaltado no es del original).

De manera que por tratarse de la aprobación de la adhesión del país a un Convenio vigente, no corresponde solicitar ni la suscripción del Acuerdo ni el otorgamiento de los Plenos Poderes, pues en este caso, la manifestación del Estado de obligarse estaría constituida por la adhesión a este instrumento y tiene los mismos efectos que la ratificación.

En el presente proyecto de ley, el texto del Convenio sobre ciberdelincuencia está debidamente traducido en el idioma español, de acuerdo con lo manifestado por la señora Katia Jiménez Pochet, Traductora e interprete Oficial del Ministerio de Relaciones Exteriores y Culto de la República de Costa Rica[73], el cual viene debidamente certificado por la señora Estela Blanco Solís Directora General a.i. de Política Exterior del Ministerio de Relaciones Exteriores y Culto, donde indica que:

"Que las anteriores treinta y tres fotocopias son fieles y exactas de la traducción oficial del inglés al español del texto del Convenio sobre Ciberdelincuencia, hecho en Budapest, el veintitrés de noviembre de dos mil uno. Se extiende la presente, para los efectos legales correspondientes, en la Dirección General de Política Exterior, a las diez horas del nueve de mayo del dos mil doce."

Por todo lo anterior, los aspectos de forma, se consideran debidamente cumplidos en relación con la Adhesión a este Convenio.

B. Competencia Parlamentaria sobre los Convenios

Una de las atribuciones que establece la Constitución Política a la Asamblea Legislativa, según el inciso 4) del artículo 121 es la de:

***"4)** Aprobar o improbar los convenios internacionales, tratados públicos y concordatos.*

Los tratados públicos y convenios internacionales, que atribuyan o transfieran determinadas competencias a un ordenamiento jurídico comunitario, con el propósito de realizar objetivos regionales y comunes, requerirán la aprobación de la Asamblea Legislativa, por votación no menor de los dos tercios de la totalidad de sus miembros.

No requerirán aprobación legislativa los protocolos de menor rango, derivados de tratados públicos o convenios internacionales aprobados por la Asamblea, cuando estos instrumentos autoricen de modo expreso tal derivación."

De manera que la competencia del Parlamento en el trámite de los instrumentos internacionales consiste en la aprobación o no de convenios internacionales, tratados públicos y concordatos; estableciendo límites al legislador de no modificar el acuerdo de voluntades entre sujetos de derecho internacional.

[73] Nombrada por Acuerdo Ejecutivo número DM 8-DJ, según se indica en el sello que imprime en todas las páginas de la traducción del Convenio en estudio.

C. Votación

De conformidad con los artículos 24[74] y 121 inciso 4) de la Constitución Política, este Convenio de Adhesión para su aprobación se requiere del total de dos tercios de los votos del Plenario Legislativo.

Además, si la Asamblea Legislativa decide apartarse del criterio de la Corte Suprema de Justicia, requiere el voto de las dos terceras partes del total de los miembros de la Asamblea Legislativa.

D. Delegación

Este proyecto de ley no puede ser delegado para su aprobación en una Comisión con Potestad Legislativa Plena por las siguientes consideraciones:

- Se encuentra en las excepciones que dispone el artículo 124 constitucional.
- Por tratarse de la aprobación un Convenio internacional es competencia exclusiva del Plenario Legislativo -artículo 121 inciso 4) constitucional-

E. Consultas

Obligatoria (157 Reglamento Asamblea Legislativa y 167 Constitución Política):

- Instituto Costarricense de Electricidad[75]

---

[74] Ver artículo 18 de la Adhesión del Convenio sobre ciberdelincuencia.

[75] Cuando no puede aplicar las medidas de obtención en tiempo real de datos de tráfico –art. 20-, o de la interceptación de datos sobre el contenido -art. 21- a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios, específicamente en lo indicado en el artículo 14 punto 3. Veamos:

"Artículo 14. Ámbito de aplicación de las disposiciones sobre procedimiento

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente sección para los fines de investigaciones o procedimientos penales específicos.

2. Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:

a. los delitos penales previstos de conformidad con los artículos 2 a 11 del presente Convenio;

b. otros delitos cometidos por medio de un sistema informático; y

c. la obtención de pruebas electrónicas de un delito.

3. a. Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.

b. Cuando, ***como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:***

ii. utilizado en beneficio de un grupo restringido de usuarios, y

iii. ***no utilice las redes públicas de comunicaciones ni esté conectado a otro sistema informático, ya sea público o privado, dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21.****"* El destacado no es del original).

- Patronato Nacional de la Infancia[76]
- Corte Suprema de Justicia [77]

Preceptiva de Constitucionalidad

De conformidad con los artículos10 inciso b)[78] de la Constitución Política, 96, inciso a)[79] y el 98[80]; de la Ley de Jurisdicción Constitucional N° 7135 del 11 de octubre de 1989, en concordancia con el artículo 144[81] del Reglamento de la Asamblea Legislativa, el

---

[76] Por los delitos relacionados con la pornografía infantil.

[77] La aprobación de la Adhesión al Convenio sobre ciberdelincuencia establece:

"**Artículo 15. Condiciones y salvaguardas**.

1. Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950) , del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

*2. **Cuando resulte procedente** dada la naturaleza del procedimiento o del poder de que se trate, **dichas condiciones incluirán**, entre otros, aspectos, **la supervisión judicial** u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.*

*3. Siempre que sea conforme con el interés particular, **con la correcta administración de la justicia**, cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros."* (El destacado no es del original)

[78] *"**Artículo 10**. Corresponderá a una Sala especializada de la Corte Suprema de Justicia declarar, por mayoría absoluta de sus miembros, la inconstitucionalidad de las normas de cualquier naturaleza y de los actos sujetos al Derecho Público. No serán impugnables en esa vía los actos jurisdiccionales del Poder Judicial, la declaratoria de elección que haga el Tribunal Supremo de Elecciones y los demás que determine la ley.*

Le corresponde además:

(…)

b) Conocer de las consultas sobre proyectos de reforma constitucional, de aprobación de convenios o tratados internacionales y de otros proyectos de ley, según se disponga en la ley."

[79] ***"ARTICULO 96**. Por la vía de la consulta de constitucionalidad, la jurisdicción constitucional ejercerá la opinión consultiva previa sobre los proyectos legislativos, en los siguientes supuestos: a) Preceptivamente, cuando se trate de proyectos de reformas constitucionales, o de reformas a la presente ley, así como de los tendientes a la aprobación de convenios o tratados internacionales, inclusive las reservas hechas o propuestas a unos u otros. b) Respecto de cualesquiera otros proyectos de ley, de la aprobación legislativa de actos o contratos administrativos, o de reformas al Reglamento de Orden, Dirección y Disciplina Interior de la Asamblea Legislativa, cuando la consulta se presente por un número no menor de diez diputados. c) Cuando lo soliciten la Corte Suprema de Justicia, el Tribunal Supremo de Elecciones o la Contraloría General de la República, si se tratare de proyectos de ley o de mociones incorporadas a ellos, en cuya tramitación, contenido o efectos estimaren como indebidamente ignorados, interpretados o aplicados los principios o normas relativos a su respectiva competencia constitucional. ch) Cuando lo solicite el Defensor de los Habitantes, por considerar que infringen derechos o libertades fundamentales reconocidos por la Constitución o los instrumentos internacionales de derechos humanos vigentes en la República."*

[80] ***"ARTICULO 98.** Cuando se trate de reformas constitucionales, la consulta deberá hacerse después de su aprobación en primer debate, en primera legislatura, y antes de la definitiva. Cuando se trate de otros proyectos o actos legislativos sujetos al trámite de emisión de las leyes, deberá interponerse después de aprobados en primer debate y antes de serlo en tercero. No obstante, cuando la Asamblea Legislativa tuviere un plazo constitucional o reglamentario para votar el proyecto, la consulta deberá hacerse con la anticipación debida, y el proyecto se votará aunque no se haya recibido el criterio de la Sala. En los demás supuestos, la consulta deberá plantearse antes de la aprobación definitiva."*

proyecto de ley debe ser consultado preceptivamente a la **Sala Constitucional una vez aprobado en Primer Debate por la Asamblea Legislativa.**

Facultativas

- Ministerio de Relaciones Exteriores y Culto
- Ministerio de Seguridad Pública
- Ministerio de Ciencia, Tecnología y Telecomunicaciones
- Ministerio de Relaciones Exteriores y Culto
- Ministerio de Justicia
- Ministerio de la Presidencia
- Ministerio de Hacienda
- Dirección General de Inteligencia y Seguridad
- Organismo de Investigación Judicial
- Ministerio Público
- Centro Judicial de Intervenciones de las Comunicaciones
- Defensoría del Consumidor
- Asociación Cámara de Infocomunicación y Tecnología (Its InfoCom)
- Cámara Costarricense de Tecnologías de Información y Comunicación (Camtic)
- Cámara de Servicios Corporativos de Alta Tecnología (Camscat)
- Colegio de Abogados
- Colegios de Periodistas
- Defensoría de los Habitantes
- Procuraduría General de la República

VI.- FUENTES[82]

A. Constitución Política

- **Constitución Política de la República de Costa Rica,** del 19 de noviembre de 1949.

B. Tratados y convenios internacionales

- **Convención de Viena sobre el Derecho de los Tratados,** Ley Nº 7615, del 24 de julio de 1996.

---

[81] ***"ARTICULO 144.- Consulta preceptiva.*** *1. El Directorio de la Asamblea hará de oficio la consulta preceptiva, en los casos del inciso a) del artículo 96 de la Ley de la Jurisdicción Constitucional. 2- El Directorio, realizada la consulta preceptiva, lo comunicará de inmediato al Plenario en el capítulo de Régimen Interior. 3.- Mediante moción de orden aprobada por el Plenario, éste podrá decidir que un proyecto determinado, no consultado por el Directorio, está dentro de los supuestos previstos en el artículo 96 inciso a). En este caso, el Directorio formulará la consulta."*

[82] Información suministrada por el Licenciado Juan Conejo Trejos. Asesor Parlamentario del Área de Investigación y Gestión Documental, del Departamento de Servicios Técnicos.

- **Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y utilización de niños en la pornografía**, Ley No 8172 de 7 de diciembre de 2001.

C. Leyes

- **Ley de la Jurisdicción Constitucional**, Nº 7135 del 11 de octubre de 1989.

- **Reforma de Varios Artículos y Modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VIII del Código Penal**, Ley N° 9048 del 6 de noviembre del 2012.

- **Código de Normas y Procedimientos Tributarios**, No.4755 de 3 de mayo de 1971.

- **Ley General de Aduanas**, No. 7557 de 20 de octubre de 1995.

- **Código Penal**, No.4573 de 4 de mayo de 1970 y sus reformas.

- **Ley de Administración Financiera de la República y Presupuestos Públicos** N° 8131 de 18 de setiembre de 2001.

- **Ley de Derechos de Autor y Derechos Conexos y sus reformas**, No.6683 de 14 de octubre de 1982.

- **Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual**, No.8039 de 12 de octubre de 2000.

D. Jurisprudencia Administrativa

- **Departamento de Servicios Técnicos**, Oficio ST N° 158-2012 J de 9 DE agosto del 2012, sobre el expediente Nº 18.382, proyecto de ley: "APROBACIÓN DE LA ADHESIÓN A LA CONVENCIÓN PARA FACILITAR EL ACCESO INTERNACIONAL A LA JUSTICIA".

- ***Departamento de Servicios Técnicos***, Oficio ST- 263-2012 J, 26 de noviembre, 2012 sobre el expediente N° 18546 proyecto de ley: *"Reforma de los tipos penales establecidos en los artículos 167, 196, 196 bis, 231, 236 y 288 del Código Penal, Ley Nº 4573, publicada en el alcance 120 de la gaceta 257 de 15 de noviembre de 1970 y sus reformas".*

- **Ministerio de Ciencia y Tecnología,** Oficio N° DM-480-MICIT-2012 del 24 de setiembre de 2012, suscrito por Alejandro Cruz Molina, Ministro de Ciencia y Tecnología.

- **Instituto Costarricense de Electricidad.** Oficio N° 256-168-2012 del 27 de setiembre de 2012, suscrito por Julieta Bejarano Hernández, Jefe División Jurídica.

- **Procuraduría General de la República**, Oficio N° OJ de 31 de octubre de 2012, suscrito por José Enrique Castro Marín, Procurador Director.

E. Expediente Legislativo

- **Expediente Legislativo** Nº 18.382 proyecto de ley: *"Aprobación de la Adhesión a la Convención para facilitar el acceso internacional a la justicia".*

- **Expediente Legislativo** Nº 18.383 proyecto de ley: *"Aprobación de la "Adhesión al Convenio sobre la obtención de pruebas en el extranjero en materia civil o comercial".*

- ***Expediente Legislativo*** N° 18546 proyecto de ley: *"Reforma de los tipos penales establecidos en los artículos 167, 196, 196 bis, 231, 236 y 288 del Código Penal, Ley Nº 4573, publicada en el alcance 120 de la gaceta 257 de 15 de noviembre de 1970 y sus reformas".*

H. Publicaciones

- **Universidad de Costa Rica**, mesa redonda *"Desconocimiento y vacíos legales facilitan la ciberdelincuencia en el país"*, organizada por la Facultad de Derecho de la Universidad de Costa Rica, en conjunto con el Departamento de Servicios Bibliotecarios, Documentación e Información de la Asamblea Legislativa. Publicada por Universia Noticias Costa Rica, el 05 de octubre de 2011. Sitio: http://noticias.universia.cr/en-portada/noticia/2011/10/05/875040/desconocimiento-vacios-legales-facilitan-ciberdelincuencia-pais.html

- **Universidad de Costa Rica,** Foro *"Tipo y naturaleza de los ciberdelitos",* como parte de unas jornadas organizadas por el Programa Sociedad de la Información y el Conocimiento (Prosic) de la Universidad de Costa Rica, publicada en el Boletín Presencia Universitaria, noviembre de 2009, por *Mayela Castillo Villachica*.

- **Universidad de Costa Rica**, Mesa redonda *"Reflexiones en torno a la nueva Ley de Seguridad Informática",* organizada por el Programa Sociedad de la Información y el Conocimiento de la Universidad de Costa Rica (Prosic). Publicación *"Expertos creen que Ley de Delitos Informáticos debe ser equilibrada en aspectos jurídicos y técnicos"*, Boletín N° 21 de agosto de 2012, Categoría: Tecnología, por Anna Georgina Velásquez Vásquez.

- **La Nación.** Artículo de Opinión "Adhesión al Convenio Europeo sobre Ciberdelincuencia", Christian Hess Araya, publicado el jueves 29 de noviembre del 2012.

VII.- ANEXO

El objetivo de este apartado es observar la evolución de la regulación de las conductas que se han tipificado en nuestro derecho interno. Para ello en cuadro comparativo[83] con la Ley 9048 "Reforma de varios artículos y modificación de la Sección VIII, denominada Delitos Informáticos y conexos, al Título VII del Código Penal, y reforma del artículo 9 de la Ley Nº 7425", expediente 18546 "Reforma de los tipos penales establecidos en los artículos 167, 196, 196 bis, 231, 236 y 288 del Código Penal, Ley Nº 4573, publicada en el Alcance 120 de La Gaceta 257 de 15 de noviembre de 1970 y sus reformas y el "Código Penal, Ley Nº 4573, de 4 de mayo de 1970 y sus reformas"; Veamos:

ANALISIS COMPARATIVO

LEY 9048 "REFORMA DE VARIOS ARTÍCULOS Y MODIFICACIÓN DE LA SECCIÓN VIII, DENOMINADA DELITOS INFORMÁTICOS Y CONEXOS, AL TÍTULO VII DEL CÓDIGO PENAL, Y REFORMA DEL ARTÍCULO 9 DE LA LEY N.º 7425", EXPEDIENTE 18546 "REFORMA DE LOS TIPOS PENALES ESTABLECIDOSENLOS ARTÍCULOS 167, 196, 196 BIS, 231, 236 Y 288 DEL CÓDIGO PENAL, LEY N.º 4573, PUBLICADA EN EL ALCANCE 120 A DE LA GACETA 257 DE 15 DE NOVIEMBRE DE 1970 Y SUS REFORMAS Y EL "CÓDIGO PENAL, LEY Nº 4573, DE 4 DE MAYO DE 1970 Y SUS REFORMAS"

Código Penal	***Ley 9048 "Reforma de Varios Artículos y Modificación de la Sección VIII, denominada Delitos Informáticos y Conexos, del Título VIII del Código Penal"*** ***PUBLICADA EL 06 DE NOVIEMBRE DEL 2012 EN LA GACETA Nº 214, ALCANCE 172***	***Reforma propuesta Expediente 18546***
	ARTÍCULO 1.- Refórmanse los artículos 167, 196, 196 bis, 209, 214, 217 bis, 229 bis y 288 del Código Penal, Ley N.º 4573, de 4 de mayo de 1970, y sus reformas. Los textos dirán:	**ARTÍCULO 1.-** Refórmanse los artículos 167, 196, 196 bis, 209, 214, 217 bis, 229 bis y 288 del Código Penal, Ley N.º 4573, de 4 de mayo de 1970, y sus reformas. Los textos dirán:
Corrupción **Artículo 167.-** Será sancionado con pena de prisión de tres a ocho años, **siempre que no constituya un delito más grave**, quien promueva o mantenga la corrupción de una persona menor de edad o incapaz, **ejecutando o haciendo ejecutar a otro u otros, actos sexuales perversos, prematuros o excesivos**, aunque la víctima consienta en participar en ellos o en verlos ejecutar. La misma pena se impondrá a quien utilice a personas menores de edad o incapaces con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos, públicos o privados, de tal índole, aunque las personas menores de edad lo consientan. *(Así reformado mediante el artículo 1° de la ley N° 8590 del 18 de julio del 2007).*	**Artículo 167.- Corrupción** Será sancionado con pena de prisión de tres a ocho años quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. **La pena será de cuatro a diez años de prisión si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz, utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque** la víctima consienta participar en ellos o verlos ejecutar."	**Artículo 167.- Corrupción** Será sancionado con pena de prisión de tres a ocho años quien mantenga o procure la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta. La pena será de cuatro a diez años de prisión, si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o

[83] Tomado del criterio del **Departamento de Servicios Técnicos**, Oficio ST- 263-2012 J, 26 de noviembre, 2012 sobre el expediente N° 18546 proyecto de ley: *"Reforma de los tipos penales establecidos en los artículos 167, 196, 196 bis, 231, 236 y 288 del Código Penal, Ley Nº 4573, publicada en el alcance 120 de la gaceta 257 de 15 de noviembre de 1970 y sus reformas".*

		verlos ejecutar.
		ARTÍCULO 2.- Agréguese el siguiente párrafo al final de los artículos 196, 196 bis, 231 y 236 de la Ley N.º 4573, que es el Código Penal:
Violación de correspondencia. ARTÍCULO 196.- Será reprimido, con prisión de **uno** a **tres** años, **quien abra o se imponga del contenido de una comunicación destinada** a otra persona, **cualquiera que sea el medio utilizado**. (Así reformado por el artículo 31 de la Ley de Registro de Documentos Privados e Intervención de Comunicaciones Nº 7425 de 9 de agosto de 1994)	**Artículo 196.- Violación de correspondencia o comunicaciones** Será reprimido con **pena de** prisión de **tres a seis años** quien, **con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos** a otra persona**. La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por:** **a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.** **b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos**.	**Artículo 196.- Violación de correspondencia o comunicaciones** Será reprimido con pena de prisión de tres a seis años quien, con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos a otra persona. La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por: **a)** Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones. **b)** Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. **En ningún caso configura delito la búsqueda, acceso, copia, recopilación, o la difusión, transmisión o publicación de datos, documentos, informaciones, noticias, reportajes, imágenes o ideas que sean de interés público o que guarden relación con asuntos de esa naturaleza.**
Artículo 196 bis.- Violación de comunicaciones electrónicas Será **reprimida** con pena de prisión de **seis meses a dos** años, **la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento,** se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe **de su destino**, **mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos.** La pena será de **uno a tres** años de prisión**, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos,** magnéticos **y telemáticos**. *(Así adicionado por Ley N° 8148 de 24 de octubre del 2001)*	**Artículo 196 bis.- Violación de datos personales** Será **sancionado** con pena de prisión de **tres a seis** años **quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos**, se apodere, modifique, interfiera, acceda, **copie, transmita**, **publique**, difunda, **recopile, in**utilice, intercepte, **retenga, venda, compre**, desvíe para un fin distinto para el que **fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes i**nformáticas o telemáticas, **o en contenedores** electrónicos, **ópticos o** magnéticos. La pena será de **cuatro a ocho** años de prisión **cuando las conductas** descritas **en esta norma:** **a) Sean** realizadas por personas encargadas **de administrar o dar** soporte **al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores** electrónicos, **ópticos o** magnéticos**.** **b) Cuando las datos sean de carácter público o estén contenidos en bases de datos públicas.**	**Artículo 196 bis.- Violación de datos personales** Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos. La pena será de cuatro a ocho años de prisión cuando las conductas descritas en esta norma: **a)** Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. **b)** Cuando los datos sean de carácter público o estén contenidos

	c) Si la información vulnerada corresponde a un menor de edad o incapaz. **d) Cuando las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona**.	en bases de datos públicas. **c)** Si la información vulnerada corresponde a un menor de edad o incapaz. **d)** Cuando las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona. **En ningún caso configura delito la búsqueda, acceso, copia, recopilación, o la difusión, transmisión o publicación de datos, documentos, informaciones, noticias, reportajes, imágenes o ideas que sean de interés público o que guarden relación con asuntos de esa naturaleza.**
Artículo 209.- Hurto agravado Se aplicará prisión de un año a **tres años**, si el valor de lo sustraído no excede de cinco veces el salario base(*), y de **uno** a diez años, si fuere **superior** a esa suma, en los siguientes casos: **1)** Cuando el hurto **fuere** sobre cabezas de ganado mayor o menor, aves de corral, productos o elementos que se encuentren en uso para explotación agropecuaria. **2)** Si fuere cometido aprovechando las facilidades provenientes de un estrago, de una conmoción pública o de un infortunio particular del damnificado. **3)** Si se hiciere uso de ganzúa, llave falsa u otro instrumento semejante, o de la llave verdadera que hubiere sido sustraída, hallada o retenida. **4)** Si fuere de equipaje de viajeros, en cualquier clase de vehículos o en los estacionamientos o terminales de las empresas de transportes. **5)** Si fuere de vehículos dejados en la vía pública o en lugares de acceso público. **6)** Si fuere de cosas de valor científico, artístico, cultural, de seguridad o religioso, cuando**,** por el lugar en que se encuentren estén destinadas al servicio, a la utilidad o a la reverencia de un número indeterminado de personas, o librados a la confianza pública. **7)** Si fuere cometido por dos o más personas. *(Así reformado por el artículo 19 de la Ley de Protección a Víctimas, Testigos y demás intervinientes en el Proceso Penal N° 8720 de 4 de marzo de 2009.)* (*) Sobre la interpretación del término "salario base", véanse las observaciones a la ley).	**<u>Artículo 209.-</u> Hurto agravado** Se aplicará prisión de uno a **nueve años** si el valor de lo sustraído no excede de cinco veces el salario base, y de **cinco** a diez años, si fuera **mayor** que esa suma, en los siguientes casos: **a)** Cuando el hurto **sea** sobre cabezas de ganado mayor o menor, aves de corral, productos o elementos que se encuentren en uso para la explotación agropecuaria. **b)** Si fuera cometido aprovechando las facilidades provenientes de un estrago, de una conmoción pública o de un infortunio particular del damnificado. **c)** Si se hiciera uso de ganzúa, llave falsa u otro instrumento semejante, o de la llave verdadera que hubiera sido sustraída, hallada o retenida, **claves de acceso, tarjetas magnéticas o dispositivos electrónicos**. **d)** Si fuera de equipaje de viajeros, en cualquier clase de vehículos o en los estacionamientos o terminales de las empresas de transportes. **e)** Si fuera de vehículos dejados en la vía pública o en lugares de acceso público. **f)** Si fuera de cosas de valor científico, artístico, cultural, de seguridad o religioso, cuando por el lugar en que se encuentren estén destinadas al servicio, a la utilidad o a la reverencia de un número indeterminado de personas, o libradas a la confianza pública. **g)** Si fuera cometido por dos o más personas	
Extorsión simple. ARTÍCULO 214.- Será reprimido con prisión de **dos** a **seis** años, el que para procurar un lucro **injusto** obligare a otro con intimidación o con amenazas graves a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.	**<u>Artículo 214.-</u> Extorsión** Será reprimido con **pena de** prisión de **cuatro a ocho** años **al** que para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero. **La pena será de cinco a diez años de prisión cuando la conducta se realice**	

	valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.	
Artículo 217 bis.- **Fraude informático** Se impondrá pena de prisión de **uno** a **diez** años **a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero**, influya en el procesamiento o el resultado de los datos de un sistema de **cómputo**, mediante programación, **empleo** de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema." *(Así adicionado por el artículo 1° de la Ley N° 8148 de 24 de octubre del 2001)*	**Artículo 217 bis.- Estafa informática** Se impondrá prisión de **tres a seis** años a quien, **en perjuicio de una persona física o jurídica, manipule o** influya **en el ingreso**, en el procesamiento o en el resultado de los datos de un sistema **automatizado de información, ya sea** mediante el uso de datos falsos o incompletos, el uso indebido de datos, **programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.** **La pena será de cinco a diez años de prisión si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.**	
Artículo 229 bis.- **Alteración de datos y sabotaje informático** Se impondrá pena de prisión de **uno** a **cuatro** años a la persona que por cualquier medio accese, *borre, suprima, modifique o* ***inutilice*** *sin autorización los datos registrados en una computadora.* ***Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático****, la pena será de tres* a seis años de prisión. Si el ***programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.*** *(Así adicionado por Ley N° 8148 de 24 de octubre del 2001)* Artículo 229 bis.- **Abandono dañino de animales** *(Anulado este artículo, en lo referente al "Abandono dañino de Animales", mediante resolución de la Sala Constitucional N° 18486-07, del 19 de diciembre del 2007.)* (**NOTA DE SINALEVI**: Mediante el artículo único de la Ley No. 8148 de 24 de octubre de 2001, se adiciona el artículo 229 Bis, que regula el delito de **Alteración de datos y sabotaje informático.** Posteriormente, mediante el inciso d) del Artículo 3 de la Ley No. 8250 de 2 de mayo de 2002, se adiciona, nuevamente, un artículo 229 Bis, el cual regula el **Abandono dañino de animales**; sin percatarse el legislador de que ya existía dicho artículo y que el mismo regulaba un delito completamente diferente al	**Artículo 229 bis.- Daño informático** Se impondrá pena de prisión de uno **a tres años al que** sin autorización **del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero**, suprima, modifique o **destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos**. La pena será de tres a seis años de prisión si la **información suprimida, modificada, destruida es insustituible o irrecuperable**.	

nuevo que se creó).		
		ARTÍCULO 3.- Refórmese el artículo 288 de la Ley N.º 4573, que es el Código Penal, para que en adelante se lea de la siguiente manera:
Espionaje. **ARTÍCULO 288**.- Será reprimido con prisión de **uno** a **seis** años, **el** que procurare u obtuviere indebidamente informaciones secretas políticas o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la Nación. (Así modificada la numeración de este artículo por el numeral 185, inciso a), de la ley No.7732 de 17 de diciembre de 1997, que lo traspasó del 286 al 288)	**Artículo 288.- Espionaje** Será reprimido con prisión de **cuatro a ocho años al** que procure u obtenga indebidamente informaciones secretas políticas o de **los cuerpos de policía nacionales,** o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la nación**, o afecte la lucha contra el narcotráfico o el crimen organizado.** **La pena será de cinco a diez años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.**	**Artículo 288.- Espionaje** Será reprimido con prisión de cuatro a ocho años **a quien obtenga indebidamente información que, conforme a la ley, el Presidente de la República decrete como Secreto de Estado**.

Código Penal	***REFORMA IMPLEMENTADA MEDIANTE LEY 9048***	
	ARTÍCULO 2.- Adiciónanse el inciso 6) al artículo 229 y un artículo 229 ter al Código Penal, Ley N.º 4573, de 4 de mayo de 1970, y sus reformas. Los textos dirán:	
Artículo 229.- Daño agravado Se impondrá prisión de seis meses a cuatro años: **1)** Si el daño fuere ejecutado en cosas de valor científico, artístico, cultural o religioso, cuando, por el lugar en que se encuentren, se hallaren libradas a la confianza pública, o destinadas al servicio, la utilidad o la reverencia de un número indeterminado de personas. **2)** Cuando el daño recayere sobre medios o vías de comunicación o tránsito, sobre puentes o canales, sobre plantas de producción o conductos de agua, de electricidad o de sustancias energéticas. **3)** Cuando el hecho fuere ejecutado con violencia en las personas o con amenazas. **4)** Cuando el hecho fuere ejecutado por tres o más personas. **5)** Cuando el daño fuere contra equipamientos policiales. *(Así reformado por el artículo 19 de la Ley de Protección a Víctimas, Testigos y demás intervinientes en el Proceso Penal N° 8720 de 4 de marzo de 2009.)*	**"Artículo 229.- Daño agravado** Se impondrá prisión de seis meses a cuatro años: […] **6)** Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos."	
	Artículo 229 ter.- Sabotaje informático Se impondrá pena de prisión de tres a seis años al 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. La pena será de cuatro a ocho años de prisión cuando: **a)** Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.	

	b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos. **c)** El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas. **d)** Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.	
	ARTÍCULO 3.- Modifícase la sección VIII del título VII del Código Penal, Ley N.º 4573, de 4 de mayo de 1970, y sus reformas; se corre la numeración de los artículos subsiguientes. El texto dirá:	**ARTÍCULO 2.-** Agréguese el siguiente párrafo al final de los artículos 196, 196 bis, 231 y 236 de la Ley N.º 4573, que es el Código Penal:
Código Penal	***REFORMA INTEGRADA MEDIANTE LEY 9048***	
SECCION VIII Disposición General Tenencia y fabricación de ganzúas y otros instrumentos. **ARTÍCULO 230.-** ANULADO por Resolución de la Sala Constitucional Nº 6410-96 de las 15:12 horas del 26 de noviembre de 1996.	**Artículo 230.- Suplantación de identidad** Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien utilizando una identidad falsa o inexistente cause perjuicio a un tercero. La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz.	
	Artículo 231.- Espionaje informático Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.	**Artículo 231.- Espionaje informático** Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio. **En ningún caso configura delito la búsqueda, acceso, copia, recopilación, o la difusión, transmisión o publicación de datos, documentos, informaciones, noticias, reportajes, imágenes o ideas que sean de interés público o que guarden relación con asuntos de esa naturaleza.**
	Artículo 232.- Instalación o propagación de programas informáticos maliciosos Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos. La misma pena se impondrá en los siguientes casos: **a)** A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.	

	b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes. **c)** A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos. **d)** A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos. **e)** A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos. La pena será de tres a nueve años de prisión cuando el programa informático malicioso: **i)** Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal. **ii)** Afecte el funcionamiento de servicios públicos. **iii)** Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi. **iv)** Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero. **v)** Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas. **vi)** Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.	
	<u>Artículo 233.-</u> Suplantación de páginas electrónicas Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet. La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.	
	<u>Artículo 234.-</u> Facilitación del delito informático Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.	
	<u>Artículo 235.-</u> Narcotráfico y crimen organizado. La pena se duplicará cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.	
	<u>Artículo 236.-</u> Difusión de información falsa	**<u>Artículo 236.-</u> Difusión de información falsa**

	Será sancionado con pena de tres a seis años de prisión quien a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones propague o difunda noticias, o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios.	Será sancionado con pena de tres a seis años de prisión quién, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios. **En ningún caso configura delito la búsqueda, acceso, copia, recopilación, o la difusión, transmisión o publicación de datos, documentos, informaciones, noticias, reportajes, imágenes o ideas que sean de interés público o que guarden relación con asuntos de esa naturaleza.**
		ARTÍCULO 3.- Refórmese el artículo 288 de la Ley N.º 4573, que es el Código Penal, para que en adelante se lea de la siguiente manera:
Espionaje. ARTÍCULO 288.- Será reprimido con prisión **de uno a seis años, el que procurare u obtuviere indebidamente informaciones secretas políticas o de seguridad concernientes a los medios de defensa o a las relaciones exteriores de la Nación.** (Así modificada la numeración de este artículo por el numeral 185, inciso a), de la ley No.7732 de 17 de diciembre de 1997, que lo traspasó del 286 al 288)		**<u>Artículo 288.-</u> Espionaje** Será reprimido con prisión de cuatro a ocho años **a quien obtenga indebidamente información que, conforme a la ley, el Presidente de la República decrete como Secreto de Estado**
	ARTÍCULO 4.- Refórmase el artículo 9 de la Ley N.º 7425, Registro, secuestro y examen de documentos privados e intervención de las comunicaciones, y sus reformas, de 9 de agosto de 1994. El texto dirá:	
ARTÍCULO 9.- Autorización de intervenciones. Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, tráfico de personas y tráfico de personas para comercializar sus órganos; homicidio calificado; genocidio, terrorismo y los delitos previstos en la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, legitimación de capitales y actividades conexas, **Nº 8204, del 26 de diciembre del 2001**. En los mismos casos, dichos tribunales podrán autorizar la intervención de las comunicaciones entre los presentes, excepto lo dispuesto en el segundo párrafo del	**<u>Artículo 9.-</u> Autorización de intervenciones** Dentro de los procedimientos de una investigación policial o jurisdiccional, los tribunales de justicia podrán autorizar la intervención de comunicaciones orales, escritas o de otro tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, cuando involucre el esclarecimiento de los siguientes delitos: **delitos informáticos o cometidos mediante la utilización de medios informáticos, electrónicos, telemáticos, ópticos o magnéticos,** secuestro extorsivo, corrupción agravada, proxenetismo agravado, fabricación o producción de pornografía, **tráfico de personas y tráfico de personas** para comercializar sus órganos, homicidio calificado, genocidio, terrorismo y los delitos previstos en la Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales **y financiamiento al terrorismo**, N.° 8204, de 26 de diciembre de 2001. En los mismos casos, dichos tribunales podrán autorizar la intervención de las comunicaciones entre los presentes, excepto lo dispuesto en el segundo párrafo del artículo 26 de la presente Ley; cuando	

artículo 26 de la presente Ley; cuando se produzcan dentro de domicilios y recintos privados, la intervención solo podrá autorizarse si existen indicios suficientes de que se lleva a cabo una actividad delictiva. *(Así reformado por Ley N° 8238 de 26 de marzo del 2002)*	se produzcan dentro de domicilios y recintos privados, la intervención solo podrá autorizarse si existen indicios suficientes de que se lleva a cabo una actividad delictiva.	

EXPEDIENTE Nª 18.484
/eeb.-