

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

San José, 27 de octubre de 2010

Nº 9651 -10

Al contestar refiérase a este # de oficio

Señor

Lic. Marco William Quesada Bermúdez, Director

Secretaría del Directorio

Asamblea Legislativa

S. D.

Morgan

REC 2010-10-27-176

Estimado señor:

Muy respetuosamente, le transcribo el acuerdo tomado por la Corte Plena, en sesión Nº 30-10 celebrada el 25 de octubre último, que literalmente dice:

“ARTÍCULO XXII

SALEN LAS MAGISTRADAS PEREIRA Y CALZADA.

El licenciado Marco William Quesada Bermúdez, Director de la Secretaría del Directorio de la Asamblea Legislativa, en oficio Nº SD-54-10-11 de 12 de octubre en curso, solicitó el criterio de esta Corte sobre el proyecto de ley denominado “Reforma a varios capítulos del Código Penal y Adición de una nueva sección denominada “Delitos Informáticos y Conexos”, al título VII del Código Penal”, expediente # 17.613.

La consulta se remitió a estudio del Magistrado Chinchilla, quien en nota de 22 de este mes, rinde el siguiente informe:

“Procedo a dar respuesta el oficio número 076-2010, remitido a este Despacho, mediante el cual se me solicitó mi criterio para informar de manera escrita, acerca del proyecto de ley denominado “*Reforma a varios capítulos del Código Penal y adición de una nueva sección denominada “Delitos Informáticos y Conexos”, al título VII del Código penal*”, expediente Nº 17.613, para efectos internos se le asignó el PL-006-10.

ASPECTOS GENERALES

Al hablar del tema de los *delitos informáticos*, resulta indispensable hacer referencia al contenido y alcances de esta temática, cuyo conocimiento y estudio se ubica en el ámbito del *Derecho Penal Económico*. De igual forma, es importante referir su evolución histórica y fundamentos dogmático-penales (en este sentido ver, CHINCHILLA SANDÍ, Carlos, *Delitos Informáticos: su relación con el Derecho*

Teléfonos: 2295-3707 al 2295-3711 Correo: secrecorte@poder-judicial.go.cr Fax: (506) 2295-3706 Apdo: 1-1003

San José

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

penal económico y el Derecho informático, San José, Editorial Norma-Farben, 2004, pp. 152).

Derecho Penal Económico

El ciberdelito es un relevante campo de la criminalidad, el cual tiene directa relación con el **Derecho Penal Económico**, ámbito que en Costa Rica es desconocido porque, lamentablemente, nunca se han desarrollado investigaciones sobre el mismo. No obstante, en Europa cuenta con poco más de veinte años de desarrollo científico y, por lo tanto, dogmático. Lo anterior provoca que, en Costa Rica, se encuentre en completo abandono, aunque poco a poco se espera una mayor difusión y exponer su verdadera importancia.

Delitos económicos

Cuando hablamos de la **ciberdelincuencia**, realizamos una directa identificación con los llamados **delitos económicos**. Estos últimos, desde el ámbito de la **criminalidad informática**, muestran una característica que los identifica singularmente, referida a la utilización de las modernas **Tecnologías de la Información y la Comunicación** (en adelante **TIC**), en medio de la llamada **Sociedad de la Información y el Conocimiento**.

Una característica relevante de estos delitos, como lo veremos, se refiere a la utilización de los llamados **delitos de peligro abstracto**, donde no se necesita la existencia de un resultado, sino, por el contrario, el ordenamiento adelanta la protección de bienes jurídicos que consideran relevantes, para sancionar la acción delictiva. Por ello, lo que hoy identificamos como la tentativa en los delitos de resultado, en los delitos de peligro, sería la verificación de un riesgo o peligro y, por lo tanto, sancionable como si se tratara del resultado mismo. Lo dicho, corresponde a la figura de los delitos de peligro abstracto.

Sociedad del riesgo

Este moderno concepto de la llamada **Sociedad del Riesgo**, no es más que el resultado del desarrollo y evolución de nuestras sociedades. Teniendo como punto de partida, para la mayoría de autores de temas sociológicos, a partir de la Revolución Industrial del siglo XVIII, iniciada en Inglaterra y expuesta a su aplicación en el resto de países europeos y el resto del mundo, hasta el día de hoy.

Esta sociedad del riesgo acentúa su interés en la generación de focos de peligro o riesgo en una sociedad, dirigidos, irremediablemente, por el avance y desarrollo en los procesos de producción. En este sentido, en los albores de su génesis, resulta evidente el cambio de la producción artesanal y por piezas individuales, a la producción en serie, donde la cantidad se impone a la individualidad; incorporándose como medio de producción efectivo y eficaz, la automatización de los procesos de producción, donde la utilización, cada vez más acentuada, de máquinas, viene a desplazar las fuerzas

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

productivas manuales o humanas. Esto genera una nueva forma de identificar las relaciones laborales y el cambio de atención hacia los medios tecnológicos en beneficio de la generación de riqueza.

Las llamadas sociedades de riesgo, muestran algunas características comunes;

Progreso y desarrollo en la sociedad, genera una serie de riesgos.

Los riesgos son asumidos socialmente.

La industrialización, el tráfico automotor, actualmente la Internet, etc.; son factores que propician la aparición de las actividades riesgosas.

La característica esencial de las sociedades modernas es, sin lugar a duda, el incremento del riesgo.

Lo anterior provoca, lamentablemente, la generación de conductas delictivas.

Este concepto de la **sociedad del riesgo**, viene a ser desarrollado por el sociólogo alemán Ulrich Beck, quien le brinda un contenido amplio y de gran actualidad. Esta sociedad del riesgo se vincula, directamente, con los avances tecnológicos y la sobrevenida sociedad de la información y el conocimiento. Todo esto tiene que ver con la sociedad del riesgo, la cual es reflejo de la actual sociedad de la información y el conocimiento, porque nuestras sociedades son altamente riesgosas y, aunque parezca mentira, entre más desarrollada sea una sociedad, más peligros genera; sin embargo, entre más rudimentaria y atrasada sea la sociedad, menos peligro produce. A pesar de ello, la solución no es devolvernos en el camino, porque las condiciones que hoy día gozan nuestras sociedades son innumerables. Por ello, lo que debemos procurar, en forma decidida, es el control de los riesgos en la sociedad, para vivir en forma más tranquila y placentera, disfrutando de los grandes avances tecnológicos.

En este sentido, el surgimiento de la Internet, así como su uso masivo, se convierte en un instrumento de progreso y desarrollo social, donde las sociedades se conectan, intercambian información y se mantienen actualizadas. Hoy día, para nadie es un secreto que la información produce actualidad, pero aún más, la información debidamente administrada y actualizada, produce conocimiento y riqueza. Lamentablemente, la Internet no es utilizada únicamente con fines de desarrollo y progreso, sino también, para generar conductas delictivas, lo cual hace percibir y conocer de una gran cantidad de peligros entre los usuarios, de esta forma de comunicación digital.

Los delitos económicos, así como los delitos informáticos, tienen mucho que ver, con la evolucionada **delincuencia organizada**. Donde poderosas organizaciones criminales se sirven de muchas personas, para cometer delitos informáticos.

Delitos informáticos

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

Cuando hablamos de **delitos informáticos**, nos referimos, por un lado, al uso de la informática y, por otro, a la necesaria utilización de las telecomunicaciones; la utilización simultánea de ambos campos de acción nos conduce a la telemática.

Tratando de buscar una definición de los delitos informáticos como, *“la acción delictiva que realiza una persona, con la utilización de un medio informático o lesionando los derechos del titular de un elemento informático, se trate de las máquinas -hardware- o de los programas -software-”* (CHINCHILLA SANDÍ, Carlos, *Delitos informáticos*, San José, Editorial Investigaciones Jurídicas S.A., 2002, p.26).

En esta definición se comprenden dos ámbitos, el primero, cuando se hace uso de un medio informático para cometer un hecho ilícito y, el segundo, cuando se vulneran los derechos de un elemento informático ya sea el software o el hardware, constituyendo una acción de carácter delictiva.

En la delincuencia informática, partimos de que se puede cometer bajo el supuesto de la acción ejecutada con dolo, lo que corresponde a que el sujeto activo cuenta con el debido conocimiento y voluntad, o, según sea el caso, con culpa o imprudencia, identificada por la infracción al deber de cuidado.

Sujetos que intervienen en los hechos delictivos informáticos.

Tenemos dos tipos de personas que intervienen en los hechos criminales informáticos; el sujeto activo y el sujeto pasivo.

Características del sujeto activo;

- No necesariamente poseen importantes conocimientos de informática.
- Ocupan lugares estratégicos en su trabajo, donde se maneja información importante y accesos restringidos a los sistemas informáticos.

El sujeto activo no necesariamente posee amplios conocimientos de informática, aunque no estamos diciendo que, muchos de ellos, cuenten con los mismos. Sin embargo, en la práctica, la mayoría de delitos informáticos son cometidos por personas que no tienen esos profundos conocimientos en informática.

Lo que no podemos dejar de lado es que, esos sujetos que no necesariamente se encuentran especializados en informática y, además, directamente ejecutan los hechos criminales. De igual forma, en no pocos casos, cuentan con el apoyo o resultan ser utilizados, por sujetos que sí cuentan con esos conocimientos. Además, podemos agregar que podrían surgir las redes criminales que funcionan con criminalidad organizada, donde ubican muchas de sus piezas en puestos o funciones claves dentro de las empresas e instituciones, para realizar actividades ilícitas.

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

Lo anterior resulta muy importante, porque estas personas ocupan un lugar estratégico en su lugar de trabajo, sea una empresa privada o institución pública, donde resultan puestos importantes, aunque no estamos hablando de jerarcas, sino de mandos medios y, algunas veces, un poco más bajos. ¿Qué es lo que se ocupa? Tener un lugar estratégico, tener acceso al sistema, entrar en lugares donde está vedado para la mayoría introducirse, y realizar sus acciones delictivas.

Se identifican como sujetos activos a los hackers; correspondiendo a una terminología que ha correspondido, en un momento histórico anterior, no a delincuente. Sin embargo, hoy día, el término hacker se refiere al delincuente informático. La acción de "hackear", o sea, introducirse sin autorización a un sistema informático o acceder a una base de datos, se había realizado por personas muy jóvenes, ubicadas en grupos etarios de los 13 a los 15 años y de los 16 a los 19. No obstante, la idea de ese joven inquieto, con gran capacidad intelectual para alcanzar conocimientos muy especializados en informática y, simplemente, vulnerar seguridades informáticas, al día de hoy, ese hacker rebasó la línea divisoria entre el simple juego, para convertirse en un delincuente informático.

Esa tentación de pasar al campo de la ilicitud, se ve favorecida por tener a su disposición, una vez que se vulneran las seguridades de acceso a los sistemas informáticos, gran cantidad de dinero electrónico, que es muy fácil de distraer y dirigir a cuentas electrónicas personales a de terceras personas que se prestan para ello. Un hacker verdadero, por su corta edad, muy probablemente no cuenta con títulos universitarios, los cuales no requiere, porque cuenta con un coeficiente mental superior al promedio, donde se identifican con niños o jóvenes genios, sin límites para su aprendizaje adelantado, donde la tecnología permite ese desarrollo. Al contrario, el hacker de hoy en día, término identificado con delincuentes informáticos, donde ha ayudado en mucho para esta conclusión, los medios de comunicación pero, indiscutiblemente, las mismas personas que realizan estas actividades, es estigmatizante y cargado de un absoluto contenido delictivo.

Características del sujeto pasivo

Es la persona o entidad sobre la cual recae la conducta que realiza el sujeto activo. La mayoría de delitos informáticos no son descubiertos porque no son denunciados por empresas o bancos, temen desprestigio y consecuente pérdida económica. Esto provoca que la llamada "cifra negra" de la criminalidad, en este tipo de delitos, sea muy elevada.

Características de los delitos informáticos

Podemos citar cuatro características comunes de los delitos informáticos;

- Rapidez; en el tiempo de ejecución. Con un simple "click" se ejecuta el hecho.

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

- Acercamiento en espacio; la ejecución del delito se realiza, muchas de las veces, por personas que forman parte de la empresa o institución perjudicada. Sin embargo, es posible que la ejecución se realice en forma remota y, por lo tanto, a larga distancia del asiento de las víctimas.

- Facilidad para encubrir el hecho; la forma como se realizan los delitos informáticos permiten, la posibilidad de encubrir el hecho, desde una perspectiva informática.

- Facilidad para borrar las pruebas o huellas informáticas. Es evidente que si quien ejecutada este tipo de acción delictiva, es una persona de amplios conocimientos informáticos, logrará la destrucción de las huellas informáticas que podrían descubrirlo. Lo anterior se potencia en sus efectos, porque al tratarse de delitos de carácter económico, donde la finalidad es lograr distraer dineros públicos o privados, la averiguación que se haga de ello por parte de los perjudicados será, lamentablemente, al menos seis meses o un año posterior a su realización. Lo anterior es así, debido a que las prácticas de auditorías externas y aún las internas, no se realizan con la frecuencia necesaria, sino, por el contrario, en el mejor de los casos, una vez cada dos años.

CONTENIDO DEL PROYECTO

Este proyecto de ley cuenta con *cuatro artículos*, los cuales se analizarán a continuación.

ARTÍCULO 1

Este primer artículo reforma los numerales 167, 196, 196 Bis.-, 209, 214, 217 Bis.-, 229 Bis.-, y 288 del Código Penal.

- **Artículo 167. Corrupción.** Se regula el delito de **Corrupción**, donde se introduce la penalización de cuatro a diez años de prisión, como conducta agravada del tipo penal base, cuando el sujeto activo utilice las redes sociales o cualquier otro medio informático o telemático para buscar encuentros de carácter sexual para sí o para otro, o para grupos, con una persona menor de edad o incapaz, o utilice a estas personas para promover la corrupción, o los obligue a realizar actos sexuales perversos.

- **Artículo 196. Violación de correspondencia o comunicaciones.** Se modifica el *nomen iuris* por el de **Violación de correspondencia o comunicaciones**, donde se sanciona con un mínimo de 3 años y hasta 6 años de prisión, donde se regula acciones que pongan en peligro o dañen 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 dirigidas a otra persona. Con ello, se brinda una más clara protección al derecho fundamental a la intimidad, previsto en el artículo 24 de la Constitución Política. Asimismo, se agrava la

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

pena de 4 a 8 años de prisión, si esas conductas las realiza el encargado de la recolección, entrega o salvaguarda de los documentos o comunicaciones o las personas encargadas de dar soporte al sistema o que tengan acceso al mismo. Lo cual comprende el uso abusivo e ilícito de las personas que deben preservar esa intimidad y violentan su deber de reserva y probidad.

- **Artículo 196 Bis. Violación de Datos personales.** En esta norma se protege el ámbito de la privacidad e intimidad, donde podemos hablar del principio de **autodeterminación informativa**. La actual disposición legal vigente, contiene algunos yerros importantes, como es el caso de la pretendida agravante final de la conducta, cuando se habla que la pena se aumentará, cuando las acciones sean ejecutadas por los encargados de los soportes, sistemas informáticos o bases de datos, y se dice en forma expresa; "*La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior*", el problema es que el legislador olvidó que este precepto legal se redactó en un único párrafo, por lo cual, no existe el "*párrafo anterior*", haciendo inaplicable esta agravante. La disposición propuesta en la presente reforma, modifica el **nomen iuris** por el de **Violación de datos personales**, donde se contempla una sanción penal de 3 a 6 años de prisión, para la persona que se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre o desvíe para un fin distinto o le de 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, en su forma agravada aumenta la pena de 4 a 8 años de prisión cuando la conducta se realice por los encargados de administrar o dar soporte al sistema, cuando los datos sean de carácter público, se vulnere la información de un menor de edad o revelen la ideología, religión, creencias, salud, origen racial, preferencia o vida sexual de una persona.

- **Artículo 209. Hurto agravado.** Se trata del delito de **Hurto agravado**, donde se modifica la numeración de los incisos para establecerlos en orden alfabético, su contenido queda igual y establece una nueva penalidad de 1 a 9 años de prisión si el valor de lo sustraído no excede de 5 veces el salario base y, si es mayor a esa suma, la penalidad se mantiene de 5 a 10 años. La sensible novedad que se introduce en esta norma, se refiere al inciso c), cuando se introduce la utilización de "**claves de acceso, tarjetas magnéticas o dispositivos electrónicos**". Con ello, se produce un sensible avance en la legislación de los delitos informáticos, pues esta conducta ha traído un grave problema de resolución por parte de los Tribunales de Justicia y la misma Sala Tercera, donde se ha llegado a discutir la subsunción de la conducta delictiva en el delito de estafa informática, hurto agravado o hurto simple. Con esta reforma, no quedará duda que la utilización delictiva de estos instrumentos de carácter informático, se considerarán hurtos agravados.

- **Artículo 214. Extorsión.** Introduce la reforma a la **Extorsión**, contemplando una sanción de prisión de 4 a 8 años y, la novedad es que agrava la pena de 5 a 10 años de prisión, cuando se realice la conducta mediante la manipulación informática, telemática, electrónica o tecnológica. Esto encuentra respaldo, por la utilización de medios tecnológicos para la comisión de acciones delictivas.

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

- **Artículo 217 Bis. Fraude informático.** Regula el llamado **Fraude informático** y sanciona en su forma base la penalidad de 3 a 6 años de prisión, al que 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. Se llega a agravar la pena de prisión de 5 a 10 años de prisión, si esas conductas se cometen contra sistemas de información públicos, bancarios o de cualquier entidad financiera o si el autor es el encargado de administrar o dar soporte al sistema o bien por razón de sus funciones tenga acceso al mismo. La reforma en su contenido ha sido muy bien pensada, debido a que se incluyen dos elementos esenciales; uno referido a la **"manipulación"** como verbo identificador de la conducta delictiva, junto con el de **"influir"** y, otro, donde se introduce la posibilidad de que las acciones defraudatorias se realicen al momento del **ingreso** de los datos al sistema, siendo que el actual artículo 217 bis del Código Penal, sobre el Fraude informático, no se contemplan estos dos elementos. Los llamados **"insiders"** o la manipulación en el ingreso de los datos, según estadísticas a nivel internacional, es donde se verifican, aproximadamente, el 80% de todas las estafas informáticas; además, se mantiene en la descripción del tipo penal, la manipulación en el **procesamiento** de los datos y el **"outsiders"** o **salida** de los datos. Estos tres momentos son los que corresponden al funcionamiento de cualquier sistema informáticos, donde los mismos se alimentan de datos o información (introducción), se procesa la misma y, por último, se da la salida de los datos. Un aspecto que no resulta especialmente esencial y no afecta para nada el contenido del tipo penal, pero sí es importante para su correcta identificación, se refiere al **nomen iuris** otorgado al artículo 217 bis del proyecto, al identificarlo como **Fraude informático**, al igual que la norma vigente hoy día. En realidad, el error de ese artículo en su nombre jurídico que mantiene actualmente, se repite en el actual proyecto de ley, cuando en realidad se debió adoptar el nombre de **Estafa informática**. En este sentido, para explicar nuestra posición, es importante aclarar que, cuando en la doctrina de los Delitos Informáticos se habla de "fraude", no es lo mismo que, cuando en la doctrina del Derecho Penal se refiere al mismo término "fraude". Con ello se quiere decir que, en delitos informáticos el concepto de "fraude" va más allá que en el Derecho Penal especial. Existe confusión entre los conceptos de fraude informático y estafa informática. Por eso podemos decir que, no es lo mismo fraude informático y estafa informática, aunque ambos se llegan a confundir; donde los fraudes informáticos constituyen el género y las estafas informáticas, son la especie. Por ello, podríamos afirmar que, *"toda estafa informática es un fraude informático, pero no todo fraude informático es una estafa informática"*. En realidad, si se revisa la doctrina acerca de los delitos informáticos, muchas veces un fraude informático puede ser un hurto informático, un sabotaje informático o un daño informático. Por ello, limitar el **nomen iuris** (nombre que se le da un delito) para ubicar su contenido, como lo podría ser el fraude informático, no resulta correcto en el presente caso, lo más apropiado sería renombrarlo como **Estafa informática**.

- **Artículo 229 Bis. Daño informático.** Se cambia su nombre a Daño Informático y el tipo penal base se sanciona con prisión de 1 a 3 años -actualmente es de 1 a 4 años de prisión- para la persona que sin el permiso del titular o excediendo sus

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

funciones y en perjuicio de tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos. Se mantiene la agravación de la pena de 1 a 6 años si la información suprimida, modificada, destruida es insustituible o irrecuperable.

- **Artículo 288. Espionaje.** Se introduce una figura novedosa y muy actual dentro del ámbito de los delitos informáticos, referida no la simple conducta de espionaje, sino aquella que tiene relación con la realizada por medio de la utilización de las modernas tecnologías de la información y la comunicación (TIC), donde se 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. El tipo base se sanciona con prisión de 4 a 8 años, además se incorporan conductas agravadas, sancionadas con prisión de 5 a 10 años, cuando la conducta se realice mediante la manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.

ARTÍCULO 2

- Se reforma el **Artículo 229. Daño agravado** del Código Penal, introduciéndole el inciso 6) para imponer pena de 6 meses a 4 años de prisión: cuando el daño recayere sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos.

- Se introduce el **Artículo 229 Ter. Sabotaje informático.** Se hace una correcta utilización de la técnica legislativa, al numerar este artículo como "**Ter**", para evitar confusiones y problemas, cuando años atrás se generaron dos simultáneos artículos 229 bis del Código Penal, el primero de ellos se refiere a la Alteración de datos y sabotaje informático y, el segundo, declarado inconstitucional por la Sala Constitucional, se dirigía a regular el llamado Abandono dañino de animales. Para evitar esta situación algo complicada, el legislador en este proyecto numera adecuadamente esta nueva disposición legal, evitando errores de identificación. El Sabotaje informático se regula en su tipo base con una sanción de 3 a 6 años de prisión, donde se penaliza a quien en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o 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. Esta conducta se agrava con una sanción de 4 a 8 años de prisión cuando, como consecuencia de la conducta del autor sobrevenga un peligro colectivo o daño social, la conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o en razón de sus funciones tenga acceso a dicho sistema, el sistema sea de carácter público o la información esté contenida en bases públicas o sin estar facultado el agente emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

ARTÍCULO 3

El **artículo 3** de este proyecto modifica la Sección VIII del Título VII del Código Penal, Ley N° 4573, del 4 de mayo de 1970 y sus reformas y corre la numeración de los artículos subsiguientes, para que se lea la nueva Sección VIII: Delitos Informáticos y Conexos, la cual contendrá los siguientes artículos:

- **Artículo 230. Suplantación de identidad.** Se sanciona con prisión de 3 a 6 años, a quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información, misma pena se impondrá a quien utilizando una identidad falsa o inexistente cause perjuicio a un tercero. La pena se agrava de 4 a 8 años de prisión, si con las anteriores conductas se causa perjuicio a un menor de edad o incapaz. Esta es una conducta penal novedosa y sumamente actual, donde se utilización redes sociales o sitios de Internet, suplantando una identidad, la cual podría pertenecer a alguna persona en específico o se creada en forma artificial. Esta constituye una regulación altamente relevante, donde se logra evitar que las personas participen simulando ser una persona determinada, sin que ello sea cierto. Lo anterior corresponde a un delito de peligro abstracto, donde se sanciona una conducta, sin necesidad de que se produzca un resultado, como efecto directo del moderno Derecho Penal Económico y la Ciberdelincuencia.
- **Artículo 231. Espionaje informático.** Esta disposición sanciona con prisión de 3 a 6 años de prisión, a quien 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. Este delito propuesto se diferencia del Espionaje del art. 288, el cual contiene también sanción por la utilización de tecnologías modernas, en que este último tiene relación directa con aspectos de seguridad nacional, crimen organizado y narcotráfico, pero en el artículo en comentario del Espionaje informático, se refiere a la conducta donde se sanciona al que se apodere e información o datos privados, con un especial valor para el tráfico económico de la industria y el comercio.
- **Artículo 232. Instalación o propagación de Programas informáticos maliciosos.** Esta norma tiene directa relación con la difusión del llamado "*malware*" o, *software o programas maliciosos*, los que generan graves problemas en los sistemas informáticos y las bases de datos, públicas o privadas. En forma específica se regula la instalación o propagación de programas informáticos maliciosos imponiendo la pena de prisión de 1 a 6 años y agravando tal pena de 3 a 9 años de prisión, cuando el programa informático malicioso: afecte una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal, afecte el funcionamiento de servicios públicos, se obtenga el control a distancia de un sistema o de una red informática, para formar parte de una red de ordenadores zombi, esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero, afecte sistemas informáticos de la salud y la afectación de los mismos pueda poner en peligro la salud o vida de las personas, o que tenga la capacidad de reproducirse sin la

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

necesidad de intervención adicional por parte del usuario legítimo del sistema informático. Este artículo en su inciso **b)** contiene un evidente error en la utilización del término “convertidos”, el cual se debe cambiar por la palabra “convertirlos”, la que resulta adecuada para la regulación legal que se pretende.

- **Artículo 233.- Suplantación de páginas electrónicas.** Esta propuesta de regulación legal contiene aspectos de especial comentario y relevancia. Se recoge en forma específica, lo relativo a las conductas del “*phishing*” y el “*pharming*”, las cuales han afectado y lesionado a muchas personas alrededor del mundo. Son actuaciones de especial actualidad, donde constantemente se verifica una gran cantidad de conductas fraudulentas, por medio de las cuales se afecta económicamente a una gran cantidad de personas, empresas e instituciones. En este artículo se impone pena de prisión de 1 a 3 años a quien en perjuicio de un tercero, suplante sitios legítimos de la red de Internet y, además, se agrava la pena de 3 a 6 años de prisión, cuando a consecuencia de esa suplantación capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

- **Artículo 234.- Facilitación del delito informático.** Esta regulación sanciona con prisión de 1 a 4 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. Esta conducta no se encuentra regulada, por lo que resulta novedosa y se identifica con el proceder de muchas personas que facilitan información, sin que actualmente se logren sancionar penalmente.

- **Artículo 235.- Narcotráfico y crimen organizado.** Esta norma recoge una agravante genérica, donde se duplica la pena, 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. Tiene su razón de existencia bajo las acciones dirigidas a entorpecer el combate al narcotráfico y el crimen organizado, por medio de la utilización de las modernas tecnologías de la información y comunicación (TIC), sancionado más severamente esas acciones por medio de la duplicación de la pena.

- **Artículo 236.- Difusión de Información Falsa,** impone pena de 3 a 6 años de prisión a 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.

ARTÍCULO 4

El **ARTÍCULO 4** de este proyecto, se dirige a modificar el **Artículo 8** de la **Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones y sus reformas, N° 7425 del 9 de agosto de 1994**, que permite la *autorización de intervenciones* introduciendo la posibilidad de los Tribunales de Justicia de autorizar las intervenciones de comunicaciones orales, escritas o de otros

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, *cuando involucre el esclarecimiento de delitos informáticos o cometidos mediante la utilización de medios informáticos, electrónicos, telemáticos, ópticos o magnéticos*, los demás delitos se mantienen incólumes.

Esta reforma resulta de vital importancia, al introducir la posibilidad de autorizar la intervención de comunicaciones cuando involucre esclarecer delitos informáticos o cometidos por medio de la utilización de las TIC.

CONCLUSIONES

Es importante tener presente que, esta propuesta de reformas penales, donde se ubica como eje central la utilización de modernas tecnologías de la información y la comunicación (TIC) y, además, se comprende el uso masivo de la Internet y redes sociales, perfila en forma muy clara, las principales necesidades de regulación legal penal que, indiscutiblemente, cualquier país desarrollado -económica y tecnológicamente- desearía tener.

Se reformulan, con gran acierto, conductas ilícitas que anteriormente necesitaban se revisadas. En este sentido, se reforma el delito de **Corrupción (art. 167)**, donde se incorpora la protección más clara y decidida de los menores de edad e incapaces, así como la realización de dicha conducta por medios informáticos y telemáticos.

De igual forma, se remozza el contenido de los delitos de **Violación de correspondencia o comunicaciones (art. 196)**, y de **Violación de datos personales (art. 196 bis)**, donde sus contenidos logran superar errores de redacción de normas hoy vigentes que, lamentablemente, en algunos casos resultan inaplicables.

Gran acierto se encuentra en el regulación novedosa del **Hurto agravado (art. 209 inciso c)**, donde se incorpora la utilización de claves de acceso, tarjetas magnéticas o dispositivos electrónicos, como instrumentos para cometer estos ilícitos penales. Con ello, se zanja la discusión acerca de la comprometida utilización de la tarjeta de crédito o débito hurtada -sustracción sin violencia o fuerza- a una persona, donde se obtiene, a su vez, el "pin" o código de acceso a la cuenta electrónica, para lograr acceder al cajero automático, y se sustrae dinero por el autor del hecho criminal. Este caso se resolvería, con esta nueva disposición, como un hurto agravado, sin discusión alguna.

El ilícito de la **Extorsión (art. 214)** cuenta con un giro importante, generando una agravante, cuando el hecho se ejecuta por medios tecnológicos.

El delito de **Fraude informático (art. 217 bis)**, actualmente se encuentra vigente en el mismo artículo, sin embargo, contiene algunos defectos que han sido subsanados en la propuesta actual. En efecto, se incorpora la acción de "**manipular**", adjunta a la de "**influir**" y, además, algo esencialmente importante, se introduce el momento de la **manipulación en el "ingreso"** de los datos, para completar el ciclo, en

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

tres fases, de los sistemas informáticos; ingreso, procesamiento y salida de la información. La sugerencia surge en cuanto al *nomen iuris*, pues en realidad estamos ante un **Estafa informática** y no ante un **Fraude informático**, por lo que su ubicación sería como un **artículo 216 bis**.

Respecto al delito de **Espionaje (art. 288)**, lo que se hace es completar su contenidos y hacerlo extensivo de otros ámbitos de protección, en cuanto a la seguridad nacional, introduciendo la lucha contra el narcotráfico y el crimen organizado. Además, se detiene a incluir el uso de medios tecnológicos en las conductas de espionaje, como una agravante. Una figura cercana es el llamado **Espionaje informático (art. 231)**, el cual obtiene su existencia, no bajo los parámetros de la seguridad nacional, sino contemplando sanciones penales para actuaciones de manipulación informática o tecnológica, donde se apropie de información de valor para el tráfico económico de la industria y el comercio.

Se llega a adicionar al delito de **Daño agravado (art. 229)** un **inciso 6)**, donde se refiere a los daños realizados contra las redes, sistemas o equipos informáticos, telemáticos o electrónicos, lógicos o periféricos.

Un delito que hoy día se encuentra vigente, pero que cuenta con algunas deficiencias en su redacción, lo constituye, el **Sabotaje informático (art. 229 Ter)**, donde se muestra una redacción más apropiada y los supuestos de su aplicación resultan más claros y efectivos. El logro importante es que se separa, definitivamente, el delito de **Daño informático (art. 229 bis)** del ilícito de **Sabotaje informático (art. 229 Ter)**, manteniendo cada uno de ellos, una identidad propia y comprensiva de conductas especializadas, ejecutadas mediante el uso de las modernas tecnologías de la información y la comunicación, donde se afecta la información (daños informáticos) o se destruye, altera, entorpece o inutiliza la información que se encuentra en bases de datos, sin contar con la autorización correspondiente. Además, se incorporan otros supuestos que agravan la sanción penal, pues las acciones se dirigen contra la información contenida en sistemas informáticos o telemáticos de carácter público.

Por medio del **ARTICULO 3** del presente **Proyecto**, se modifica la **Sección VIII** del **Título VII** del **Código Penal**, la cual comprende artículos nuevos en sus contenidos, a partir del **artículo 230 Suplantación de identidad** y hasta el **artículo 236 Difusión de información falsa**. Lo anterior obliga a correr la numeración de los artículos subsiguientes de citado Código Penal.

El ilícito de **Suplantación de identidad (art. 230)**, representa una norma de suma actualidad y brinda respuesta, hoy día, a la gran cantidad de situaciones riesgosas que se verifican en las redes sociales y sitios de Internet. La utilización de redes sociales es una conducta normal y, podríamos decir, masificada en nuestro medio, donde la interacción es sumamente fluida y provoca la generación de relaciones cibernéticas importantes. Por ello, la necesidad de regular estos encuentros digitales, donde lo que inicialmente cuenta es una identidad y, lamentablemente, presumimos que es verdadera sin necesidad de corroboración alguna. Por ello, esta norma brinda un

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

margen de regulación adecuada para aquellos que intervienen en estas redes sociales aparentando ser otras personas, adquiriendo un perfil que no le pertenece y, lógicamente, confundiendo a sus contactos o amigos cibernautas. Esta situación se presenta como peligrosa, de ahí, la necesaria regulación penal.

El comentario del **Espionaje informático (art. 231)**, se realizó líneas atrás.

Surge un nuevo delito, identificado bajo el *nomen iuris* de **Instalación o propagación de Programas informáticos maliciosos (art. 232)**. Dicha norma se relaciona directamente con la conducta criminal de la difusión del llamado "*malware*" o, *software o programas maliciosos*, los que generan graves problemas en los sistemas informáticos y las bases de datos, públicas o privadas. Este artículo en su inciso **b)** contiene un evidente error en la utilización del término "*convertidos*", el cual se debe cambiar por la palabra "*convertirlos*", la que resulta adecuada para la regulación legal que se pretende. Esta conducta ha causado graves problemas y enormes perjuicio económicos a nivel nacional e internacional, donde se regulación, hasta el día de hoy en nuestro país, es inexistente.

El ilícito de **Suplantación de páginas electrónicas (art. 233)**, es un tipo penal nuevo. Surge como respuesta a conductas lesivas realizadas en nuestro país, cuando no se tenía regulación penal sobre ellas. La posibilidad de suplantar páginas electrónicas o *web*, genera una conducta altamente riesgosa, la cual podría llegar a desembocar en actuaciones propios de extorsión o estafas, siempre de carácter informático. Sin esta regulación legal, por el respeto del principio de legalidad que se recoge en nuestra Constitución Política en el artículo 39, no se podrían sancionar conductas de este tipo, resultando esencial su regulación, como ahora se pretende. El tipo penal propuesto se compone de dos párrafos, en el primero de ellos se regula la suplantación simple de un sitio *web* legítimo de la red de Internet. Por su parte, el segundo párrafo recoge conductas más específicas y, además, lesivas. Se trata, entre otras alternativas, de las conductas del "*phishing*" y el "*pharming*", las cuales han afectado y lesionado a muchas personas alrededor del mundo. Son actuaciones de especial actualidad, donde constantemente se verifica una gran cantidad de conductas fraudulentas, por medio de las cuales se afecta económicamente a personas, empresas e instituciones.

El delito de **Facilitación del delito informático (art. 234)**, no se encuentra regulado, por lo que resulta novedosa y se identifica con el proceder de muchas personas que facilitan información, sin que actualmente se logren sancionar penalmente.

Por su parte, el ilícito de **Narcotráfico y crimen organizado (art. 235)**, recoge una agravante genérica, donde se duplica la pena, 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. Tiene su razón de existencia bajo las acciones dirigidas a entorpecer el combate al narcotráfico y el crimen organizado, por medio de la utilización de las

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

modernas tecnologías de la información y comunicación (TIC), sancionado más severamente esas acciones por medio de la duplicación de la pena.

Por último, el **ARTÍCULO 4** de este proyecto, se dirige a modificar el **Artículo 8** de la **Ley de Registro, Secuestro y Examen de Documentos Privados e Intervención de las Comunicaciones y sus reformas, N° 7425 del 9 de agosto de 1994**, que permite la *autorización de intervenciones* introduciendo la posibilidad de los Tribunales de Justicia de autorizar las intervenciones de comunicaciones orales, escritas o de otros tipo, incluso las telecomunicaciones fijas, móviles, inalámbricas y digitales, *cuando involucre el esclarecimiento de delitos informáticos o cometidos mediante la utilización de medios informáticos, electrónicos, telemáticos, ópticos o magnéticos*, los demás delitos se mantienen incólumes. Esta reforma resulta de vital importancia, al introducir la posibilidad de autorizar la intervención de comunicaciones cuando involucre esclarecer delitos informáticos o cometidos por medio de la utilización de las TIC. Esta reforma mantiene, como siempre ha sido, la **obligatoria intervención de los Tribunales de Justicia (Juez Penal o de Garantías)**, para *decidir acerca de la autorización* o no, respecto a la intervención de las comunicaciones. Como vemos, le corresponde a un **Juez Penal de la República**, decidir si procede o no, la intervención de las comunicaciones solicitada en una investigación criminal dirigida por el Ministerio Público. Esta es una facultad de carácter jurisdiccional, otorgada y protegida bajo reserva legal calificada, conforme el artículo 24 de la Constitución Política.

Sanciones penales:

Respecto al tema de las sanciones penales que se consignan en los diferentes tipos penales, se debe decir que, de las 17 normas penales que se generan, 15 de ellas contienen una sanción penal de tres años o menos de prisión, en sus tipos base. Lo que permite la aplicación de medidas alternativas que se regulan en el Código Procesal Penal, como lo son, la conciliación (art. 36 CPP), suspensión del procedimiento a prueba (art. 25 CPP), reparación integral del daño (art. 30 inciso j. CPP), así como la posibilidad del procedimiento abreviado, el cual no es propiamente una medida alternativa, pero sí permite llegar a una sentencia condenatoria en forma anticipada, por medio de un procedimiento sumario.

Únicamente se cuenta con dos delitos, donde el extremo inferior de la pena supera los tres años de prisión, tal es el caso de la **Extorsión (art. 214)** y el **Espionaje (art. 288)**. En ambos casos, la pena inferior del tipo base se establece en cuatro años de prisión, por lo que no sería posible la aplicación de las medidas alternativas de la conciliación y la suspensión del procedimiento a prueba; no obstante, subsiste la posibilidad de la reparación integral del daño -según los medios de ejecución utilizados- y el procedimiento abreviado.

No obsta indicar que, en el caso de los dos delitos referidos, se trata de conductas altamente lesivas y graves. En el caso de la **Extorsión**, se compromete la libertad de decisión y disposición de la persona, donde se le obliga a tomar una

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

disposición patrimonial injusta a favor de su agresor o un tercero, donde prevalece la intimidación o las amenazas graves como medios de ejecución. Respecto al delito de **Espionaje**, al ser una conducta altamente censurable, donde se provoca la vulneración de los más altos bienes jurídicos, como lo son, la "**seguridad nacional**" y la "**lucha contra el narcotráfico y el crimen organizado**", merece una protección especial, reflejada en la sanción penal propuesta.

Debe quedar claro que la Asamblea Legislativa cuenta con la potestad de generar la política criminal que se requiere para nuestro país, de ahí que, estos comentarios acerca de los montos de las sanciones penales, se realizan con la intención de poder ofrecer algunos insumos, para el momento de tomar la decisión final en el plenario legislativo.

Como apreciación de fondo, se debe decir que la aprobación de este novedoso Proyecto de Ley de regulación de los Delitos Informáticos, por parte de la Asamblea Legislativa, resultaría sumamente conveniente, donde colocaría a Costa Rica como uno de los países más avanzados de Latinoamérica y, podríamos decir, del mundo, en cuanto al reconocimiento de la aplicación de las modernas Tecnologías de la Información y la Comunicación (TIC) y su regulación legal desde el ámbito del Derecho Penal.

En definitiva, el presente informe brinda un dictamen positivo, hacia un Proyecto de Ley que reúne elementos muy importantes y necesarios para combatir la **cibercriminalidad**, donde sus propuestas de reforma resultan asertivas y convenientes de regulación de acciones criminales no convencionales, donde el crimen organizado, será el mayor afectado.

En la forma anteriormente expuesta, dejo rendido mi informe."

- 0 -

Interviene el Magistrado Cruz: "Quiero hacer una observación de algo que a mí me ha preocupado. Desconozco si estará resuelto en la política criminal de persecución de muy diversa índole, porque veo que también incide en el tema de las intervenciones de comunicaciones. Yo no sé si ahí está resuelto algo que puede surgir y ha surgido con la transnacionalización de los crímenes, referente a qué pasa cuando las órdenes de intervención de comunicaciones o de documentos los da una autoridad que no es un juez en otro país. Quisiera saber si eso está o no resuelto. Solamente es una inquietud, porque veo que hay como una intendencia a incorporar una visión transnacional del tema, pero también hay particularidades de cada país en relación a esto. Yo recuerdo en situaciones muy especiales un caso como el de Panamá, donde también se hacen las intervenciones por orden del fiscal. Creo que eso es importante que hubiera estado dilucidado. Es muy probable que no lo esté. Desde la visión de crimen organizado eso debiera estar previsto. Observo que se reglamentan muchos aspectos que actualmente son anomia, pero supongo que eso no está previsto, porque nosotros tenemos una visión muy judicializada de todos esos temas."

Responde el Magistrado Chinchilla: "El Magistrado Cruz tiene mucha razón en lo que dice. En algunas ocasiones intervino en la Comisión y la preocupación era que nadie más que el juez podía hacerlo,

Teléfonos: 2295-3707 al 2295-3711 Correo: secrecorte@poder-judicial.go.cr Fax: (506) 2295-3706 Apdo: 1-1003
San José

República de Costa Rica
Corte Suprema de Justicia
Secretaría General

partiendo de la excepcionalidad del artículo 24 de la Constitución Política y la reserva legal especial, porque requiere una votación calificada para poder llegar a definir quién es el que puede ejecutarla. La preocupación era si podían los fiscales y si podían agencias externas ni siquiera públicas, sino privadas contratadas para que lo realizaran. Los señores Diputados optaron por mantener lo que se regula en la Constitución Política y lo que señala la Ley de Intervenciones en este caso. Me parece que es un debate que debería hacerse a nivel más amplio, por ejemplo, a nivel latinoamericano o centroamericano, para poder implementar algunos mecanismos necesarios para regular, porque no necesariamente todas las legislaciones tienen la misma protección como la tenemos nosotros desde el ámbito, pero se mantuvo como siempre se ha tenido.”

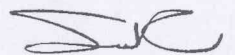
Expresa el Magistrado Arroyo: “Quiero que se me aclare una duda. Este informe se pronuncia diciendo esto es parte de lo que la Asamblea Legislativa puede hacer dentro de sus competencias, pero a la vez se le da un aval, un respaldo. Si es o no un asunto que tenga que ver con la organización y funcionamiento del Poder Judicial y en qué calidad se le estaría dando un aval al informe.”

Indica el Presidente, Magistrado Mora: “Lo que yo entiendo es que en este caso estamos diciendo que el proyecto de ley analizado en sí no afecta la organización y funcionamiento del Poder Judicial y que esta Corte avala se tramite por ser algo propio de la Asamblea Legislativa.”

Se acordó: Tener por rendido el informe del Magistrado Chinchilla, y con la observación hecha por el Presidente, Magistrado Mora, acogerlo como propio de esta Corte y hacerlo de conocimiento del licenciado Marco William Quesada Bermúdez, Director de la Secretaría del Directorio de la Asamblea Legislativa, en respuesta a la consulta formulada.

Los Magistrados Armijo, Cruz, Castillo y el Suplente Hernández Gutiérrez se abstuvieron de votar. **Se declara acuerdo firme.** ”

De usted atentamente,



Licda. Silvia Navarro Romanini
Secretaria General
Corte Suprema de Justicia

CC: Diligencias
Ref.:10890, 11281-10
Ashley