Señor Presidente:

Han venido para dictamen de la Comisión de Justicia y Derechos Humanos los **Proyectos de Ley 034/2011-CR**, presentado por el Grupo Parlamentario Alianza por el Gran Cambio, a iniciativa de los señores congresistas: Juan Carlos Eguren Neuenschwander, Luis Ibérico Núñez, Javier Bedoya de Vivanco, Luis Galarreta Velarde, Lourdes Alcorta Suero y Gabriela Pérez del Solar Cuculiza; y, **307/2011-CR**, presentado por el Grupo Parlamentario Fujimorista, a iniciativa de los señores congresistas: Octavio Salazar Miranda, Luz Salgado Rubianes, Alejandro Aguinaga Recuenco, Luisa María Cuculiza Torre, Julio Rosas Huaranga y Carlos Tubino Arias Schreiber, mediante los cuales proponen la Ley que regula los delitos informáticos.

I. CONTENIDO DE LOS PROYECTOS DE LEY

En el **Proyecto de Ley 034/2011-CR** se propone una ley especial de represión de los delitos informáticos que afectan los sistemas informáticos (la informática como objeto) y los supuestos de uso de sistemas informáticos que lesionan otros bienes jurídicos y que no puedan reprimirse satisfactoriamente con los tipos penales contenidos en el Código Penal (la informática como medio), como por ejemplo: la indemnidad sexual, el patrimonio, la fe pública, y propiedad intelectual; estableciendo medidas de derecho penal general y disposiciones procesales especiales para la mejor represión de estos delitos. Para este efecto, contiene un glosario de términos técnicos.

En el **Proyecto de Ley 307/2011-CR** se propone la protección integral de los sistemas que utilicen tecnologías de información y define nuevas figuras delictivas, algunos alcances sobre el secreto de las comunicaciones y secreto bancario, con la finalidad de facilitar el acceso a la información y otorgar facultades a la Policía Nacional del Perú y al Ministerio Público durante la investigación de hechos delictuosos.

II. MARCO NORMATIVO

- Constitución Política del Perú: artículo 2 numerales 5, 6 y 7; y artículo 97.
- Código Penal: artículos 207-A, 207-B y 207-C.
- Ley 27309, Ley que incorpora los delitos informáticos al Código Penal, publicada el 17.07.2000.

III. ANÁLISIS DE LA PROPUESTA LEGISLATIVA

a. Análisis técnico

Las actividades criminales que implican el delito informático ha llevado a que la legislación pretenda encuadrarlas dentro de figuras típicas tradicionales, tales como el robo, el hurto, los fraudes, las falsificaciones, las estafas, los sabotajes, etc. Sin embargo, dado el uso de las técnicas informáticas para su comisión ha creado la necesidad de regulación por parte del derecho.

Por tanto, regular las implicaciones de la informática en el fenómeno delictivo resulta una cuestión actual y necesaria para quienes observan el impacto de las nuevas tecnologías en el ámbito social y jurídico. En efecto, la masificación de las nuevas tecnologías de la información ha

dado lugar a debates y cuestiones, tales como el análisis de la suficiencia del sistema jurídico actual para regular las nuevas posiciones, los nuevos escenarios, en donde se debaten los problemas del uso y abuso de la actividad informática y su repercusión en el mundo contemporáneo. Es por esta razón que se requiere regular estas nuevas conductas teniendo en consideración el avance de la tecnología informática y su influencia en casi todas las áreas de la vida social. Han surgido una serie de **comportamientos** antes impensables y en algunos casos de difícil tipificación en las normas penales tradicionales, sin recurrir a aplicaciones analógicas prohibidas por el principio de legalidad.

Al respecto, el doctor Santiago Acurio del Pino en su libro Delitos informáticos: generalidades" señala que "*Los progresos mundiales de las computadoras, el creciente aumento de la capacidad de almacenamiento y procesamiento, la miniaturización de los chips de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "**era de la información**", a lo que con más propiedad, podríamos decir que más bien estamos frente a la "**era de la informática**"".*

En consecuencia, la doctrina ha denominado a este grupo de comportamientos, de manera genérica, "**delitos informáticos, criminalidad mediante computadoras, delincuencia informática, criminalidad informática"**. En este contexto, se hace necesario conocer algunos aspectos generales de esta clase de delitos. Así se tiene:

1. Antecedentes normativos internacionales

1977: La primera propuesta legislativa del delito informático es introducida por el senador Ribicoff en el Congreso Federal de Estados Unidos. En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE), en París, designó un comité de expertos para discutir el crimen relacionado con las computadoras y la necesidad de cambios en los códigos penales. Como resultado, la OCDE recomendó incorporar en las legislaciones penales para incorporar ciertas categorías de delitos informáticos.

1983: La OCDE inició un estudio sobre la posibilidad de armonizar las leyes penales en el plano internacional y publicó en 1986 un informe, llamado: Delitos de informática: análisis de la normativa jurídica, con las recomendaciones sobre cuales serían los usos indebidos que los distintos países podrían prohibir y sancionar a través de sus leyes penales.

1989: El Consejo de Europa convocó a otro comité de expertos, que en la Recomendación número (89) 9 adoptada el 13 de septiembre de 1989 presenta una lista mínima de los delitos sobre los que debía necesariamente legislarse en cada país miembro, y una lista opcional.

1990: El problema fue también discutido en el Décimo Tercer Congreso Internacional de la Academia de Derecho Comparado, realizado en Montreal en 1990; en el Octavo Congreso Criminal de las Naciones Unidas, celebrado en La Habana el mismo año y en la Conferencia de Wurzburgo, Alemania, en 1992.

1995: El Consejo de Europa adopta en Septiembre de 1995, otra recomendación concerniente a los problemas de derecho procesal conectados con la información tecnológica.

1996: El Comité Europeo para los Problemas de la Delincuencia (CDPC) decidió en noviembre de 1996 establecer un nuevo comité de expertos para que se abordara el caso de los delitos informáticos. Debido a que el ciberespacio puede ser utilizado con fines legítimos pero también puede ser objeto de un mal uso, ya sea contra la integridad, la disponibilidad y la confidencialidad de los sistemas informáticos y las redes de telecomunicaciones o su uso para cometer delitos tradicionales. El carácter transfronterizo de dichos delitos, está en conflicto con la territorialidad de las autoridades nacionales encargadas de hacer cumplir las leyes. Por ello, el derecho penal debe mantenerse actualizado con los desarrollos tecnológicos que ofrecen oportunidades altamente sofisticadas para hacer un mal uso de las facilidades del ciberespacio y perjudicar intereses legítimos.

2004: Entra en vigencia el Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre del 2001 por el Comité de Ministros del Consejo de Europa en su sesión 109, el cual, a la fecha, es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia, a saber aspectos relacionados al derecho penal, derecho procesal penal y asunto de cooperación internacional en la investigación, persecución y juzgamiento de esta clase de *delitos.*

2. Definición de los delitos informáticos

El proyecto de ley pretende legislar los vacíos del Código Penal vigente sobre la penalización de los delitos cometidos mediante conocimientos informáticos y que afectan diversos bienes jurídicos tutelados, esto es, los delitos pluriofensivos, por lo que se necesita de una ley específica para esta clase de ilícitos penales.

No hay una definición formal y universal del delito informático pero se han formulado conceptos que responden a realidades nacionales concretas:

El **Departamento de investigación de la Universidad de México** define los delitos informáticos como todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

La **Organización para la Cooperación Económica y el Desarrollo (OCED**) lo define como: "cualquier conducta no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos". Precisamente, de acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a PARIS en Mayo de 1983, el término ***delitos relacionados con las computadoras*** se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

Para **Julio TELLEZ VALDEZ**[1] los delitos informáticos son "actitudes ilícitas que tienen a las computadoras como instrumento o fin" (concepto atípico) o las "conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin" (concepto típico)."

Asimismo, el tratadista penal italiano **Carlos Sarzana di S. Ippoli**[2] , quien en su lengua materna definió a los delitos informáticos de la siguiente manera:

[1] TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996 Pág. 103-104

[2] *SARZANA DI S. IPPOLITO, Carlo "Informatica, Internet e diritto penale", Terza Ediziones, p.57, Giuffré Editore, Italia, año 2010.*

> "In altre parole puó dirsi che il computer-crime, in senso proprio, riguarda qualsiasi fatto o atto ilegale, contrario alle norme penali, nel quale il computer è stato coinvolto como oggeto del fatto o como strumento o come simbolo."[2]

Esta expresión se traduce al castellano de la siguiente manera:

> *"En otras palabras, podría decirse que el delito informático, en sentido propio, se refiere a cualquier hecho o acto ilícito, contrario a la ley penal, en el que la computadora está involucrada como objeto del hecho, como instrumento o como símbolo."*

En el Perú, se ha preferido optar por incorporar a los delitos informáticos dentro del cuerpo del Código Penal, mediante un capítulo específico para el tratamiento de los delitos informáticos (Capítulo X) que incorporó los artículos 207-A, 207-B y 207-C. Ello por la Ley 27309, que incorpora dichos delitos en nuestra codificación penal, clasificándolos como delitos contra el patrimonio.

3. Descripción de los delitos informáticos

3.1 Clasificación según la actividad informática

A. Sabotaje informático

El término sabotaje informático comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.

- **Conductas dirigidas a causar daños físicos**

  El primer grupo comprende todo tipo de conductas destinadas a la destrucción "física" del hardware y el software de un sistema. En general, estas conductas pueden ser analizadas, desde el punto de vista jurídico, en forma similar a los comportamientos análogos de destrucción física de otra clase de objetos previstos típicamente en el delito de daño.

- **Conductas dirigidas a causar daños lógicos**

  El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos "lógicos", o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

  Este tipo de daño a un sistema se puede alcanzar de diversas formas, que van desde desenchufar el ordenador mientras se está trabajando con la consiguiente pérdida de documentos, archivo o datos, hasta la utilización de los más complejos programas lógicos destructivos.

B. Fraude mediante computadoras

Este fraude consistente en la manipulación ilícita, por la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas. Así, es posible alterar, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador. También es posible interferir en el correcto procesamiento de la información, alterando el programa o la secuencia lógica con el que trabaja el ordenador, sea modificando programas originales o adicionando programas especiales. Por último, es posible falsear el resultado, inicialmente correcto, obtenido por un ordenador: a esta modalidad se la conoce como manipulación del output.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos, que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.), que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles.

C. Estafas electrónicas

La proliferación de las compras telemáticas permite que aumenten también los casos de estafa. Se trataría en este caso de una dinámica comisiva que cumpliría todos los requisitos del delito de estafa, ya que además del engaño y el «animus defraudandi» existiría un engaño a la persona que compra. No obstante seguiría existiendo una laguna legal en aquellos países cuya legislación no prevea los casos en los que la operación se hace engañando al ordenador.

D. "Phishing" o "pesca" de claves secretas

Los sabuesos suelen engañar a los usuarios nuevos e incautos de la Internet para que revelen sus claves personales haciéndose pasar por agentes de la ley o empleados del proveedor del servicio. Los delincuentes utilizan programas para identificar claves de usuarios, que más tarde se pueden usar para esconder su verdadera identidad y cometer otras fechorías, desde el uso no autorizado de sistemas de computadoras hasta delitos financieros, vandalismo o actos de terrorismo.

E. Estratagemas

Los estafadores utilizan diversas técnicas para ocultar computadoras que se "parecen" electrónicamente a otras para lograr acceso a algún sistema generalmente restringido y cometer delitos.

F. Juegos de azar

El juego electrónico de azar se ha incrementado a medida que el comercio brinda facilidades de crédito y transferencia de fondos en la red. Los problemas ocurren en países donde ese juego es un delito o las autoridades nacionales exigen licencias. Además, no se puede garantizar un juego limpio, dadas las inconveniencias técnicas y jurisdiccionales que entraña su supervisión.

G. Fraude

Se han hecho ofertas fraudulentas al consumidor tales como la cotización de acciones, bonos y valores o la venta de equipos de computadora en regiones donde existe el comercio electrónico.

H. Blanqueo de dinero

Se espera que el comercio electrónico sea el nuevo lugar de transferencia electrónica de mercancías o dinero para lavar las ganancias que deja el delito, sobre todo si se pueden ocultar transacciones.

I. Copia ilegal de software y espionaje informático

Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información. Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

J. Infracción de los derechos de autor

La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca diferencias de criterio a nivel jurisprudencial.

K. Uso ilegítimo de sistemas informáticos ajenos

Consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometido por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo.

L. Delitos informáticos contra la privacidad

Se refiere a quien, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o cualquier otro tipo de archivo o registro público o privado.

También se comprende la interceptación de las comunicaciones, la utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, se piensa que entre lo anterior se encuentra el pinchado de redes informáticas.

M. Pornografía infantil

La distribución de pornografía infantil por todo el mundo a través de la Internet está en aumento. Durante los pasados cinco años, el número de condenas por transmisión o posesión de pornografía infantil ha aumentado de 100 a 400 al año en un país norteamericano. El problema se agrava al aparecer nuevas tecnologías, como la criptografía, que sirve para esconder pornografía y demás material «ofensivo» que se transmita o archive.

3.4 Sujeto activo del delito

En este orden de ideas, las personas que cometen los "delitos informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos. Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "ingresa" en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente informático es asunto de controversia ya que para algunos el nivel de *aptitudes* no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos. Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los delitos informáticos, los estudiosos en la materia los han catalogado como delitos de cuello blanco, frase introducida por primera vez por el criminólogo norteamericano Edwin Sutherland[3] en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como delitos de cuello blanco, aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros. Asimismo, este criminólogo estadounidense dice que tanto la definición de los delitos informáticos como la de los delitos de cuello blanco no son de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos se tiene que:

> *«El sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional».*

Es difícil elaborar estadísticas sobre ambos tipos de delitos. Sin embargo, la cifra es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos «respetables» otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

---

[3] **Edwin H. Sutherland** (* 1883-1950) fue un sociólogo estadounidense. Está considerado como uno de los criminólogos más influyentes del siglo XX. Fue un sociólogo de la escuela interaccionista simbólico de pensamiento y es muy conocido por la definición de asociación diferencial, que es una teoría general del delito y la delincuencia que explica cómo desviados llegado a aprender las motivaciones y los conocimientos técnicos o desviados para actividades delictivas. Sutherland obtuvo su PhD. en Sociología, de la Universidad de Chicago en 1913 y presidió la American Sociological Association en 1939.

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes. Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas. Por su parte, en el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos se señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de que tipo de conductas deben constituir delitos informáticos.

- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

- Falta de especialización de las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

- Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

En este sentido, es destacable que la delincuencia informática se apoya en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora, aunque no es el único medio. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente aun en países latinoamericanos, conlleva también a la posibilidad creciente de estos delitos; por eso puede señalarse que la criminalidad informática constituye un reto considerable tanto para los sectores afectados de la infraestructura crítica de un país, como para los legisladores, las autoridades policiales encargadas de las investigaciones y los funcionarios judiciales.

3.5 Sujeto Pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

En primer término tenemos que distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera, que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo de los delitos informáticos para conocer los diferentes ilícitos que cometen los delincuentes informáticos con el objeto de prever las acciones por parte de los operadores de justicia debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

3.6 Bien jurídico protegido

La doctrina establece que los delitos informáticos afectan al bien jurídico información (en cualquiera de las formas: desde mensajes de datos hasta sistemas informáticos complejos) cuya protección adecuada y eficaz ante la posibilidad de ser alterada, modificada, copiada o manipulada en forma indebida, para salvaguardar su confidencialidad, integridad y/o disponibilidad para sus legítimos usuarios, genera a su vez confianza en la informática como instrumento que favorece el desarrollo humano y que contribuye a mejorar la calidad de vida de la población.

3.7 Riesgos que exponen al sistema financiero

Evidentemente que el artículo que es más atractivo de robar es el dinero o algo de valor. Por ello, los sistemas más expuestos al fraude son los que tratan pagos, como los de nómina, ventas, o compras. En ellos es donde es más fácil convertir transacciones fraudulentas en dinero y sacarlo de la empresa.

Por razones similares, las **empresas integrantes del sistema financiero** y las compañías de seguros están más expuestas a fraudes que las demás. Los sistemas mecanizados son susceptibles de pérdidas o fraudes debido a que:

- Tratan grandes volúmenes de datos e interviene poco personal, lo que impide verificar todas las partidas.

- Se sobrecargan los registros magnéticos, perdiéndose la evidencia auditable o la secuencia de acontecimientos.

- A veces los registros magnéticos son transitorios y a menos que se realicen pruebas dentro de un período de tiempo corto, podrían perderse los detalles de lo que sucedió, quedando sólo los efectos.

- Los sistemas son impersonales, aparecen en un formato ilegible y están controlados parcialmente por personas cuya principal preocupación son los aspectos técnicos del equipo y del sistema y que no comprenden, o no les afecta, el significado de los datos que manipulan.

- En el diseño de un sistema importante es difícil asegurar que se han previsto todas las situaciones posibles y es probable que en las previsiones que se hayan hecho queden huecos sin cubrir. Los sistemas tienden a ser algo rígidos y no siempre se diseñan o modifican al ritmo con que se producen los acontecimientos; esto puede llegar a ser otra fuente de agujeros.

- Solo parte del personal de proceso de datos conoce todas las implicaciones del sistema, y el centro de cálculo puede llegar a ser un centro de información. Al mismo tiempo, el centro de cálculo procesará muchos aspectos similares de las transacciones.

- En el centro de cálculo hay un personal muy inteligente, que trabaja por iniciativa propia la mayoría del tiempo y podría resultar difícil implantar unos niveles normales de control y supervisión.

- El error y el fraude son difíciles de equiparar. A menudo, los errores no son iguales al fraude. Cuando surgen discrepancias, no se imagina que se ha producido un fraude, y la investigación puede abandonarse antes de llegar a esa conclusión. Se tiende a empezar buscando errores de programación y del sistema. Si falla esta operación, se buscan fallos

técnicos y operativos. Solo cuando todas estas averiguaciones han dado resultados negativos, acaba pensándose en que la causa podría ser un fraude.

En consecuencia, si se tiene en cuenta que los sistemas informáticos pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como bancarias, financieras, tributarias, previsionales y de identificación de las personas, se deben regular estas situaciones en una nueva norma especial.

Adicionalmente, si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares se comprenderá que están en juego o podrían llegar a estarlo de modo dramático algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico institucional debe proteger.

En este caso, la humanidad no está frente al peligro de la informática sino frente a la posibilidad real de que individuos o grupos sin escrúpulos, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a expensas de las libertades individuales y en detrimento de las personas. Asimismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo.

Estas distintas medidas de protección no tienen porqué ser excluyentes unas de otras, sino que, por el contrario, estas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática solo mediante una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

3.8 Los delitos informáticos en la legislación penal peruana.

Los delitos informáticos se encuentran incorporados en nuestra legislación penal desde el año 2000, a partir de la promulgación de la Ley 27309 que los incluyó dentro del Código Penal, específicamente como una categoría de delitos contra el patrimonio. Si partimos de la premisa de que el derecho penal es una herramienta no innovativa sino que tiene su razón de ser en la realidad preexistente, la normalidad debería apuntar a una aplicación profusa de la referida norma a partir de su promulgación y entrada en vigencia, más aun si consideramos que la norma tiene once años de vigencia.

Sin embargo, la realidad determina que el ordenamiento penal referido a los delitos informáticos se ha caracterizado precisamente por la escasa aplicación de la que ha sido objeto por parte de los agentes operadores del derecho penal, vale decir, abogados, policía, fiscalía y judicatura, tal como lo revelan las estadísticas publicadas por el Ministerio Público. Esta lamentable situación ha aumentado la vulnerabilidad del Perú frente a la amenaza de la cada vez más tecnificada delincuencia informática, sobre todo si se considera que los países del entorno latinoamericano vienen tomando medidas para protegerse, siguiendo el criterio establecido por las Naciones Unidas, o bien por la Convención de Budapest.

Si se toma en cuenta que la Ley 27309 incorporó a la legislación peruana referida a los delitos informáticos únicamente a las figuras de sabotaje, intrusismo y sus correspondientes agravantes y que, como ya se ha comentado, a pesar de su antigüedad esta ley casi no registra aplicación en las estadísticas oficiales, cabe concluir que el Perú no solamente tiene considerable retraso

frente a otras realidades extraterritoriales, sino que, principalmente, evidencia una situación agobiante, caótica y apremiante frente a este fenómeno criminal. La regulación deficiente que exhibe el Perú, aunada a la excesiva lentitud del proceso de adopción de las modificaciones necesarias para modernizar el marco legal que permita combatir los delitos informáticos con mayor prolijidad, solamente beneficia a la delincuencia que opera en el país y desde territorios extranjeros, en perjuicio de las personas y empresas que no solamente caen cada vez más en estado de zozobra, sino que también se ven obligadas a invertir mayores recursos para protegerse de una amenaza creciente prácticamente sin la ayuda del Estado.
Por esta razón, hoy en día urge la incorporación de modificaciones a la ley penal peruana, por lo que, desde nuestra perspectiva, si bien es cierto que el proyecto de ley bajo comentario tiene el carácter de perfectible, también lo es que en el fondo todo proyecto de norma o inclusive las propias normas aprobadas y en vigencia también lo son. Como bien lo recoge en su propio texto, el proyecto actualiza la iniciativa legislativa multipartidaria 3083/2008-CR la cual no solamente se encuentra casi íntegramente reproducida y recogida en el anteproyecto de código penal elaborado por la Comisión de Justicia y Derechos Humanos en el quinquenio legislativo anterior, sino que, además del consenso político, también tenía la opinión favorable del Ministerio de Justicia y de los representantes del Poder Judicial y del Ministerio Público. La búsqueda del perfeccionamiento legal no puede condicionar la existencia de una herramienta legal que, sin duda alguna, traerá más beneficios que inconvenientes, en la medida que sea prontamente aprobada y sancionada.

En consecuencia, a partir de la promulgación de la Ley 29733, Ley de protección de los datos personales, hecho posterior a la iniciativa legislativa 3083/2008-CR, actualizada por el proyecto de ley materia del presente comentario, consideramos que resulta necesario otorgar a dicho instrumento legal aún por reglamentarse, de la suficiente fortaleza conceptual, estructurada sobre la base del estándar normativo europeo de protección de datos personales, con influencia de la aplicación concreta de la norma especial española. Así pues, dado este cambio en el panorama de la realidad legal, sugerimos que el artículo 8 del proyecto sea suprimido, a efectos de no entrar en controversia legal con la regulación recientemente en vigencia, la cual ya tipifica una serie de infracciones y establece las correspondientes sanciones administrativas.

Precisamente, a tenor de las propuestas formuladas en los Proyectos de Ley 034/2011-CR y 307/2011-CR, se recibió aportes de los especialistas en derecho penal y en tecnología de la información y propiedad intelectual, doctores. Álvaro Javier Thais Rodríguez y Ruddy Medina Plasencia, respectivamente, quienes ha formulado los aportes técnico-jurídicos que han permitido perfeccionar las fórmulas legales propuestas por los autores de las iniciativas legislativas materia del presente dictamen.

3.9 Del texto sustitutorio de la Comisión

En nuestro país se advierte que el ordenamiento jurídico en materia penal no ha avanzado en estos últimos tiempos a diferencia de otras legislaciones antes citadas, por lo que, tratándose del sistema punitivo peruano, se hace necesaria su regulación mediante una ley especial.

En este contexto, la iniciativa legislativa materia de análisis busca sistematizar mediante una ley especial todas las conductas ilícitas que se encuentran relacionadas con el manejo y utilización de sistemas informáticos y, por lo tanto, contribuir a una mejor tipificación penal, lo que a su vez contribuye a la oportuna persecución y sanción a quienes cometen delitos informáticos en perjuicio de diversos bienes jurídicos protegidos.

El capítulo I, entre otros aspectos, contiene un glosario de términos que contribuye a definir con mayor precisión cada una de las nomenclaturas que se utilizan en la norma a fin de evitar que se les asigne significados disimiles.

En el capítulo II se prevé la sanción de otros delitos, como el de sabotaje informático, prestación de equipos y servicios con fines de intrusismo o sabotaje y el espionaje informático.

En los capítulos III y IV se configuran los delitos de la violación del secreto de las comunicaciones y la revelación indebida de data o información de carácter personal. Estas figuras tienen estrecha vinculación con la protección constitucional a la información personal que se encuentra consagrada en el artículo 2 inciso 6) de la Constitución Política del Perú, y que, a su vez, se relaciona con el derecho a la autodeterminación informativa.

Sin embargo, se considera no regular el caso de violación de la intimidad de la data personal, que se encontraba en el artículo 8 del Proyecto de Ley 034/2011, en razón de que este asunto ya se encuentra regulado en la Ley 29733, publicada el 3 de julio de 2011 en la sección de normas legales del diario Oficial El Peruano, la cual dispone en su Título VII una serie de infracciones y sanciones administrativas.

Por otro lado, el Poder Judicial con acierto advierte que merece especial atención el contenido del artículo 10 del proyecto de ley, pues dicho dispositivo recoge una norma similar a la que estaba siendo regulada en el Proyecto de Ley 04899-2010, presentado en su momento por el Poder Judicial que proponía la modificación del 162 del Código Penal, referido a la interceptación, interferencia y difusión de comunicaciones privadas, el mismo que fue injustamente objeto de severos cuestionamientos mediáticos y por un sector de la clase política que motivaron el retiro del citado proyecto. Precisamente, estableciendo un marco garantista similar al previsto en el derecho comparado ante situaciones similares, la iniciativa del Poder Judicial, que habilitaba al juez, según las circunstancias, a exonerar de pena al agente cuando, desde un razonado criterio de proporcionalidad, resultase evidente que este había actuado en interés de causa pública o para evitar o denunciar la comisión de un delito perseguible de oficio, preocupante es entonces que el artículo 10° del proyecto vigente no hace esa distinción, estableciendo que la difusión será sancionada aún cuando el agente no hubiese tomado parte en la comisión de los delitos allí tipificados. En consecuencia el Poder Judicial señala que la figura penal contenida en la norma que se viene proponiendo resulta siendo más gravosa para quien incurre en difusión de datos o de información que haya sido objeto de interceptación violando el secreto de las comunicaciones, que aquella que se encontraba plasmada en el proyecto propuesta por el Poder Judicial. Por lo que recomiendan reformular la planteado en el Congreso y, en tal caso, acoger lo planteado por el Poder Judicial. Lo cual se ha aceptado respecto al texto legal del artículo 10º.

El capítulo V describe otras conductas punibles como la tenencia y tráfico de material de pornografía infantil, el hurto de tiempo, fraude informático, manejo fraudulento y apropiación de medios electrónicos de pago, entre otras variantes. Estos delitos ya son reprimidos por la mayoría de las legislaciones penales del mundo, por la gran incidencia que tienen en la moral pública, y además por formar parte de las políticas del Estado en defensa de la niñez.

Los Capítulos VI y VII están referidos a los delitos informáticos contra la fe pública en las modalidades de falsificación de documento informático, falsificación de tarjetas inteligentes y delitos informáticos contra la propiedad intelectual. Es indudable que tales conductas afectan gravemente el tráfico comercial que se realiza por medios de pago electrónicos de pago y necesariamente deben ser reprimidas. En tal sentido, en coincidencia con lo expresado por el Poder Judicial las normas contenidas en la propuesta legislativa son acertadas.

En cuanto a los agravantes de las conductas tipificadas, así como las penas y consecuencias accesorias se encuentran regulados en el Capítulo VIII, al igual que lo relacionado con la colaboración eficaz. Precisamente, dentro de las conductas agravadas destacan aquellas que se configuran cuando el agente activo actúa como parte integrante de una organización ilícita o cuando el delito es cometido mediante el ejercicio abusivo o ventajoso de una posición especial de acceso a la data o información reservada. Obviamente esta figura podría darse cuando el agente desempeña cargos ejecutivos o directivos que le confieren autoridad o mando sobre los sistemas informáticos de acceso restringido.

El Proyecto de Ley 034/2011-CR, materia de análisis, también incorpora la figura de la colaboración eficaz, permitiendo la reducción de la pena hasta por debajo del mínima legal cuando se trate de los autores del delito o incluso la exención de la pena si se tratase de los partícipes.

Adicionalmente, cabe precisar que el artículo 25 contempla, además de las penas principales, la imposición de penas accesorias que buscan inhabilitar al condenado para ejercer funciones o empleos públicos hasta por un periodo de tres alias. La misma pena se prevé para el ejercicio de profesión, arte o industria cuando el delito se ha cometido en el ejercicio privado de la profesión u oficio.

El secreto e inviolabilidad de las telecomunicaciones constituyen una de las garantías de preservación de la libertad personal, de la intimidad de las personas y también sirven de base para el ejercicio de otros derechos y libertades, motivo por el cual requiere de especial protección por parte de la ley. Sin embargo, esta protección no debería sobredimensionarse más allá de lo estrictamente necesario para preservar la confidencialidad del contenido de las comunicaciones, habida cuenta de que un paraguas legal protector muy amplio puede ser aprovechado por la ciberdelincuencia para incrementar la fortaleza de sus propias barreras de defensa, pero no ante la posibilidad de vulneración de sus derechos y libertades, sino ante la investigación que realizan la Policía Nacional del Perú y el Ministerio Público para denunciar la comisión de delitos informáticos.

Los datos relacionados con el número de protocolo de Internet (IP) que tienen en su poder las empresas proveedoras de servicios de Internet (PSI) permiten identificar la ubicación física de la conexión a la red y la identidad del titular a nombre de quien esta se encuentra registrada. El rápido acceso a esta información resulta de vital importancia para la investigación de delitos informáticos que realiza la policía, ya que esto incrementa las posibilidades de intervenir a los delincuentes en plena comisión del hecho delictivo y hasta de frustrar el hecho. Sin embargo, creemos que equiparar la falta de entrega de la información referida al número IP con la figura del encubrimiento real no se ajusta a la naturaleza de la conducta sancionada por el artículo 405 del Código Penal, en tanto que la demora en la entrega de esta información no es lo mismo que procurar la desaparición de las huellas o pruebas del delito ni ocultar los efectos del mismo. Por la razón expuesta, se considera pertinente eliminar la referencia al artículo 405 del Código Penal.

En el texto legal propuesto en el Proyecto de Ley 307/2011-CR se incorpora la participación de la Policía Nacional del Perú, de conformidad con lo establecido en la Ley 27934, para intervenir en los casos en los que haya tomado conocimiento de la comisión de un delito informático, teniendo la facultad de recoger y conservar los medios que se hayan utilizado rara falsificar, copiar o alterar medios electrónicos de pago, CPU o cualquier medio técnico análogo para perpetrar delitos informáticos.

El capítulo IX contiene las disposiciones procesales que regulan la intervención y control de las comunicaciones y documentos privados, la incautación de instrumentos e información sobre el

delito y la reserva de la investigación. Sin embargo, de acuerdo con la opinión del Poder Judicial el articulo 29 podría encontrar algún tipo de reservas al autorizar a la policía para incautar objetos y equipos que encuentre en el lugar de los hechos materia de intervención, pese a que esta disposición contravendría frontalmente lo dispuesto en el artículo 2 inciso 10 de la Constitución Política del Perú, norma que no permite la incautación si no es por mandato de juez competente. En este sentido, se ha incluido al fiscal y se agrega en la redacción de la fórmula legal la frase "previa orden judicial" a fin de evitar cuestionamientos de índole constitucional.

No obstante ello, cabe señalar que el valor de los medios probatorios de la comisión de un delito debe ser preservado en todas las etapas del proceso de investigación, inclusive más allá de la finalización del proceso judicial, dado que, aun bajo condena, los sentenciados podrían pedir la revisión de su causa a mérito de nuevas pruebas, las que deberán compulsarse con las que sirvieron de base a la sentencia. No creemos que resulte apropiado equiparar a los medios probatorios con aquellos otros que resultan necesarios para cumplir con la obligación de reparar civilmente el delito, ya que perder la prueba que sustenta una decisión judicial podría significar un alto impacto en el costo-beneficio de esta norma. Asimismo, el tratamiento legal para la incautación de especies ya está previsto por el artículo 24 del predictamen objeto del presente trabajo. Por esta razón, respetuosamente se considera que se desestime la inclusión de este artículo en el texto final.

Adicionalmente, se prevé incluir una disposición complementaria para modificar el artículo 1 de la Ley 27697, modificada por el Decreto Legislativo 991, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.

Finalmente, la primera disposición final deroga el inciso 3 del segundo párrafo del artículo 186 y los artículos 207-A, 207-B, 207-C del Código Penal. Tales artículos están referidos a la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general o la violación del empleo de claves secretas y a los delitos informáticos en general.

IV. LEGISLACIÓN COMPARADA

Un análisis de las legislaciones que se han promulgado en diversos países evidencia que las normas jurídicas que se han puesto en vigor están dirigidas a proteger la utilización abusiva de la información reunida y procesada mediante el uso de computadoras.

La mayoría de los países europeos ha hecho todo lo posible para incluir dentro de la ley la conducta punible penalmente, como el acceso ilegal a sistemas de cómputo o el mantenimiento ilegal de tales accesos, la difusión de virus o la interceptación de mensajes informáticos.

En la mayoría de las naciones occidentales existen normas similares a las existentes en los países europeos. Todos estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.

Para este efecto, se puede citar en la Legislación comparada la regulación siguiente:

a) Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030), que modificó al Acta de Fraude y Abuso Computacional de 1986, con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, y en qué difieren de los virus. Esta acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas

informáticos, a las redes, información, datos o programas. Es un adelanto porque está directamente en contra de los actores de transmisión de virus. Diferencia el tratamiento de aquellos que, de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos.

Constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa a la persona que defraude a otro mediante la utilización de una computadora o red informática.

b) Alemania

Este país sancionó en 1986 la Ley contra la criminalidad económica, que contempla los siguientes delitos:

• Espionaje de datos, estafa informática, alteración de datos y sabotaje informático.

c) Austria

La Ley de Reforma del Código Penal, aprobada el 22 de diciembre de 1987, en el artículo 148 sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.

d) Gran Bretaña

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (ley de abusos informáticos). Mediante esta ley, el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización. Los virus están incluidos en esa categoría. El liberar un virus tiene penas desde un mes hasta cinco años, dependiendo del daño que causen.

e) Holanda

El 1 de marzo de 1993 entró en vigencia la ley de delitos informáticos, en la cual se penaliza el hacking, el preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio), la ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría), y la distribución de virus.

La distribución de virus está penada de distinta forma si se escaparon por error o si fueron liberados para causar daño. Si se demuestra que el virus se escapó por error, la pena no superará el mes de prisión; pero si se comprueba que fueron liberados con la intención de causar daño, la pena puede llegar hasta los cuatro años de prisión.

f) Francia

En enero de 1988, este país dictó la Ley relativa al fraude informático, la cual prevé penas de dos meses a dos años de prisión y multas de diez mil a cien mil francos por la intromisión fraudulenta que suprima o modifique datos.

Asimismo, esta ley establece en su artículo 462-3 una conducta intencional y a sabiendas de estar vulnerando los derechos de terceros, se haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos. Por su parte el artículo 462-4 también incluye en su tipo penal una conducta intencional en el sentido de que, a sabiendas de estar vulnerando los derechos de terceros, en forma directa o indirecta, se haya introducido datos en un sistema de procesamiento automatizado o haya suprimido o modificado los datos que este contiene, o sus modos de procesamiento o de transmisión.

También la legislación francesa establece un tipo doloso y pena el mero acceso, agravando la pena cuando resultare la supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

Por esta ley en su artículo 462-2, se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la pena correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

g) España

En el *Nuevo Código Penal* de España, el artículo 264-2 establece que se aplicará la pena de prisión de uno a tres años y multa a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos. Sanciona en forma detallada esta categoría delictual (violación de secretos/espionaje/divulgación), aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa y cuando el hecho es cometido por funcionarios públicos se penaliza con inhabilitación.

En materia de estafas electrónicas, en su artículo 248, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en *el* caso de la comisión del delito.

h) Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993.

Según esta ley, la destrucción o inutilización de los datos contenidos dentro de una computadora es castigada con penas desde un año y medio hasta *cinco* años de prisión. Asimismo, dentro de esas consideraciones *se* encuentran los virus.

Esta ley prevé en el artículo 1 el tipo legal vigente de una conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento. En tanto, el artículo tipifica la conducta maliciosa *que* altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.

i) Argentina

La Ley 26.388, Ley de delitos informáticos, incorpora al Código Penal sanciones 'sobre la distribución y tenencia con fines de distribución de pornografía infantil, la violación de correo electrónico, el acceso ilegítimo a sistemas informáticos, el daño informático y la distribución de virus, el daño informático agravado y la interrupción de comunicaciones.

V. OPINIONES SOLICITADAS

5.1 Poder Judicial

El Presidente de la Corte Suprema de Justicia remite el Oficio N° 6745-2011-SG-CS-PJ mediante el cual opina sobre la viabilidad de la propuesta y formula aportes que han sido recogidos en los artículos 10 y 29 inciso 1 de la iniciativa legislativa materia de análisis.

5.2 Doctor Ruddy Medina Plasencia[4], especialista en tecnología de la información y propiedad Intelectual.

Remite Carta s/n del 13 de octubre de 2011, en la cual emite opinión sobre el predictamen de la Comisión de Justicia y Derechos Humanos recaído en el Proyecto de Ley 034/2011-CR, por el que se propone la ley de los delitos informáticos.

5.3 Doctor Álvaro Javier Thais Rodríguez, especialista en derecho penal y asesor legal de la Subgerencia de Tecnologías de la Información y de Seguridad de ASBANC.

El 3 de noviembre de 2011 remite ssugerencias respecto a las propuestas contenidas en los Proyectos de Ley 034/2011-CR y 307/2011-CR, que propone el texto sustitutorio de la ley de delitos informáticos.

5.4 Ministerio de Justicia

Remite Oficio 053-2012-JUS/DM, del 20 de Enero del 2012, mediante el cual comparten la propuesta que formula la dación de una ley especial sobre delitos cometidos con el uso de las tecnologías de la información y comunicaciones. Propuesta sobre la que recae un Pre Dictamen de la Comisión de Justicia y Derechos Humanos.

5.5 ASBANC

Remite Carta CO126-2011-GG-ASBANC, del 18 de octubre de 2011, mediante el cual formulan sugerencias respecto al Proyecto de Ley 34/2011-CR, precisando que resulta necesario que el proyecto de ley sea complementado en una etapa posterior para incorporar disposiciones relativas a la tentativa y complicidad y a la cooperación internacional. Asimismo, recomiendan que la Comisión impulse la aprobación de la suscripción de la Convención de Budapest (CETS 185).

5.6 Policía Nacional del Perú – División de Investigación de Delitos de Alta Tecnología

Remite Oficio N° 7574-2011-DIRINCRI-PNP/DIVINDAT-SEC, del 30 de noviembre de 2011, mediante el cual recomienda algunas modificaciones al Proyecto de Ley alcanzado por la Comisión.

[4] Abogado de Iriarte y Asociados. Information Technology& Intellectual Property Attorneys

VI. CONCLUSIÓN

En atención a las consideraciones expuestas la Comisión de Justicia y Derechos Humanos recomienda la **APROBACIÓN** de los **Proyectos de Ley 034/2011-CR y 307/2011-CR**, de conformidad con lo establecido en el literal b) del artículo 70° del Reglamento del Congreso, con el siguiente texto sustitutorio:

TEXTO SUSTITUTORIO

El Congreso de la República
Ha dado la Ley siguiente:

LEY DE LOS DELITOS INFORMÁTICOS

CAPÍTULO I

GENERALIDADES

Artículo 1: Objeto de la Ley

La presente Ley tiene el objeto de sancionar penalmente las conductas de las personas que afectan de manera relevante la información como instrumento que favorece el desarrollo humano y que contribuye a mejorar la calidad de vida de la población.

Artículo 2º.- Glosario de Términos

En la presente Ley, se emplean los siguientes conceptos:

a) Componentes de un sistema informático: Comprenden los diferentes elementos de hardware y software necesarios para el funcionamiento de sistemas y tecnologías de información.

b) Data o información: Conjunto de datos contenidos en un sistema informático, integrados, no volátiles y variables en el tiempo, que están orientados a un determinado ámbito (organización, empresa, etc.).

d) Medio electrónico de pago: Instrumento que puede utilizar una persona para realizar operaciones financieras o administrativas sobre cuentas activas o pasivas de la que es titular, por ejemplo, la compensación económica por un bien o servicio recibido. Los medios electrónicos de pago son, entre otros, las tarjetas de crédito y de débito, su representación en sistemas informáticos, así como los dispositivos electrónicos que los puedan contener.

e) Sistema informático: Conjunto de partes que funcionan relacionándose entre sí con el objetivo de capturar, almacenar y procesar información.

f) Tarjeta inteligente: Es cualquier tarjeta con circuitos integrados incluidos que permiten la ejecución de cierta lógica programada.

g) Tecnología de información: Comprende los aspectos relacionados con el hardware de un sistema informático, el cual comprende computadoras, servidores, equipos de

comunicación y equipos de seguridad, así como sistemas que permiten su operación y que son necesarios para su funcionamiento.

CAPÍTULO II
DELITOS CONTRA LOS SISTEMAS DE INFORMACIÓN Y LAS TECNOLOGÍAS DE INFORMACIÓN

Articulo 3: Intrusismo informático

El que sin estar autorizado acceda, intercepte o interfiera un sistema informático, red, datos informáticos o señales electromagnéticas, será reprimido con pena privativa de la libertad no menor de uno ni mayor de tres años.

Artículo 4: Sabotaje informático

El que sin autorización, destruya, borre, dañe, modifique o realice cualquier acto que altere, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos contenidos en el, o a una red de telecomunicaciones, será reprimido con pena privativa de la libertad no menor de uno ni mayor de seis años.

El que con fines ilícitos diseñe, desarrolle, trafique, venda, ejecute, programe o envié páginas electrónicas, enlaces o ventanas emergentes, con la finalidad de obtener información de claves de acceso y/o datos personales será sancionado con pena privativa de la libertad no menor de dos ni mayor de cinco años.

El que produzca, adquiera, distribuya, venda, introduzca o extraiga del territorio nacional software maliciosos u otros programas informáticos para cometer daños informáticos, serán sancionados con pena privativa de la libertad no menos de cuatro ni mayor de ocho años de pena privativa de la libertad.

Artículo 5: Intrusismo o sabotaje de un sistema informático con medidas de seguridad o información especial

La pena privativa de la libertad será no menor de cuatro ni mayor de siete años si los delitos previstos en los artículos 3 y 4 recaen sobre cualquiera de los componentes de un sistema informático protegido por medidas de seguridad, que estén destinados a funciones públicas o servicios privados y contengan información personal o patrimonial reservada sobre personas naturales o jurídicas.

Artículo 6: Software y Hardware empleados para intrusismo o sabotaje
El que sin estar autorizado, produzca, posea, adquiera, distribuya, envíe, diseñe, desarrolle, venda, ejecute, utilice hardware o software destinados al intrusismo o sabotaje informático de cualquier sistema informático o el que ofrezca o preste servicios que contribuyan a ese propósito, será reprimido con pena privativa de la libertad no menor de uno ni mayor de tres años.

Artículo 7: Espionaje informático

El que indebidamente obtiene, revela o difunde la data o información contenido en un sistema informático, en una tecnología de información o en cualquiera de sus componentes es reprimido con pena privativa de la libertad no menor de uno ni mayor de seis años.

La pena privativa de la libertad es no menor de tres ni mayor de siete años si el delito se comete con el fin de obtener algún tipo de beneficio para sí o para otro.

La pena privativa de la libertad es no menor de cuatro ni mayor de diez años si, a consecuencia de dicho acto se pone en peligro la seguridad del Estado, la confiabilidad general de las operaciones financieras o administrativas de las instituciones públicas o privadas afectadas, o resulta algún daño relevante para las personas naturales o jurídicas.

CAPÍTULO III

DELITOS INFORMÁTICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES

Artículo 8: Comercialización de Base de Datos

El que sin tener autorización, ofrezca, venda, intercambie, envíe, difunda, compre, intercepte, modifique o emplee información de carácter personal contenida en archivos, bases de datos o medios informáticos, electrónicos o telemáticos , o medios semejantes, será reprimido con pena privativa de la libertad no menor de uno ni mayor de cuatro años.

Artículo 9: Violación del Secreto de las Comunicaciones

El que, sin estar autorizado, mediante el uso de las Tecnologías de la información y comunicación acceda, capture, revele, difunda, ingrese, venda, compre, divulgue, intercambie, copie, intercepte, interfiera, reproduzca, modifique, desvíe o elimine, o de uso indebido, se apodere, a cualquier mensaje de datos o señal de transmisión o comunicaciones ajenas, será reprimido con pena privativa de la libertad no menor de dos ni mayor de cinco años.

Si estos hechos fueron cometidos con fines de lucro, o para facilitar la comisión de otro delito, será sancionado con una pena privativa de la libertad no menos de cuatro ni mayor de ocho años.

CAPITULO IV
DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO

Artículo 10 Hurto de tiempo

El que, sin autorización del titular o excediéndose del tiempo autorizado por éste, usa un sistema de información o una tecnología de información, es reprimido con pena privativa de la libertad no mayor de dos años si se produce un perjuicio superior a una remuneración mínima vital.

Artículo 11: Hurto informático

El que, para obtener provecho para sí o para otro, se apodera de bienes o valores tangibles o intangibles de carácter patrimonial, mediante el acceso, interceptación, o interferencia a través de cualquier sistema de información o tecnología de información, será reprimido con pena privativa de la libertad no menor de cuatro ni mayor de ocho años cuando el valor del bien o de los valores sea superior a una Remuneración Mínima Vital.

Artículo 12: Fraude informático

El que, manipulando una Tecnología de la información y comunicación, cualquiera de sus componentes o la data o información en ellos contenida, intente insertar o inserte instrucciones falsas o fraudulentas que produzcan un perjuicio ajeno, es reprimido con pena privativa de la libertad no menor de uno ni mayor de seis años.

Artículo 13: Obtención indebida de bienes o servicios

El que, utiliza sin autorización un medio electrónico de pago ajeno para obtener indebidamente cualquier efecto, bien o servicio o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida es reprimido con pena privativa de la libertad no menor de cuatro ni mayor de ocho años

Artículo 14: Manejo fraudulento de medio electrónico de pago

Es reprimido con pena privativa de la libertad no menor de cinco ni mayor de diez años el que sin autorización realiza cualquiera de las siguientes acciones.

a. Crea, captura, graba, copia, altera, duplica o elimina por cualquier medio la data o información contenida en un medio electrónico de pago.

b. Crea, duplica o altera mediante el uso de una tecnología de información, la data o información en un sistema de información con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifica la cuantía de estos.

c. Adquiere, comercializa, posee, distribuye, vende o realiza cualquier tipo de mecanismo de intervención de medios electrónicos de pago o de la data o información contenida en ellos o en un sistema de información.

Artículo 15: Apropiación de medio electrónico de pago

El que se apropia de un medio electrónico de pago que se haya perdido, extraviado o le haya sido entregado por equivocación, y lo usa, vende, o transfiere a una persona distinta del usuario autorizado o entidad emisora es reprimido con pena privativa de la libertad no menor de tres ni mayor de seis años.

La misma pena se impone a quien adquiere o recibe el medio electrónico de pago a que se refiere el primer párrafo.

Artículo 16: Provisión indebida de bienes o servicios

Sera reprimido con pena privativa de la libertad no menor de cinco ni mayor de diez años, el que sin estar debidamente autorizado realice las siguientes conductas:

1.- Cree, grabe, use, venda, compre, copie, adquiera, altere, duplique, distribuya, trasmita o elimine por cualquier medio la información contenida en los medios electrónicos de pago.

2.- Cree, grave, duplique, distribuya, adquiera, venda, compre, copie , use o altere la información contenida en un sistema informático, red, o base de datos con el objeto de incorporar usuarios, cuentas registros, o modifique la cuantía de estos.

Artículo 17: Posesión de equipo informático para falsificación de medio electrónico de pago

El que, sin estar debidamente autorizado para fabricar, emitir o distribuir medios electrónicos de pago, recibe, adquiere, posee, custodia, distribuye, transfiere, comercializa o vende cualquier equipo de fabricación de estos medios de pago o cualquier equipo o componente que captura, graba, copia, o transmite la data o información de dichos medios de pago es reprimido con pena privativa de la libertar no menor de tres ni mayor de cinco años.

CAPÍTULO V
DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA

Artículo 18: Falsificación de documento informático

Es reprimido con pena privativa de la libertad no menor de dos ni mayor de seis años el que, a través de cualquier medio, realiza sin la debida autorización y perjudicando a otro, cualquiera de las siguientes acciones:

a. **Modifica o elimina un documento que se encuentre incorporado en un sistema de información o en una tecnología de información.**

b. **Crea, modifica o elimina datos de un documento que se encuentre incorporado en un sistema de información o en una tecnología de información.**

c. **Incorpora a un sistema informático un documento ajeno a estos.**

Cuando el agente hubiera actuado con el fin de procurar para sí o para otro algún tipo de beneficio o hubiera producido un perjuicio efectivo a otro, la pena es privativa de la libertad no menor de tres ni mayor de siete años.

Artículo 19: Falsificación de tarjetas inteligentes

El que, sin autorización, crea, captura, graba, copia o duplica la data o información contenida en una tarjeta inteligente, es reprimido con pena privativa de la libertad de no menor tres ni mayor de cinco años.

La misma pena se impone al que use la data o información o una tarjeta inteligente que la contiene obtenida por otro mediante las acciones mencionadas en el primer párrafo.

CAPÍTULO VI
DELITOS INFORMÁTICOS CONTRA LOS DERECHOS DE AUTOR

Artículo 20: Reproducción de obra sin autorización

El que, con la finalidad de obtener un provecho económico, reproduce, copia, modifica, distribuye o divulga sin autorización del titular un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema informático o base de datos, es reprimido con pena privativa de la libertad no menor de cuatro ni mayor de seis años.

CAPITULO VII
DISPOSICIONES COMUNES

Artículo 21: Agravantes

Las penas correspondientes a los delitos previstos en la presente Ley a sus agravantes se incrementan en un tercio por encima del marco penal máximo en los siguientes casos:

a. **Si el agente lo comete en calidad de integrante de una organización ilícita dedicada a este tipo de delitos.**
b. **Si el agente lo comete haciendo uso de información privilegiada obtenida en función de su cargo.**
c. **Cuando atenta contra Servicios Públicos Esenciales.**
d. **Cuando atenta contra entidades financieras.**
e. **Cuando atenta contra la Seguridad Nacional.**

<u>Artículo 22:</u> Penas accesorias

Además de las penas previstas en los capítulos II, III, IV, V y VI, se impone, la inhabilitación en los siguientes casos:

a. **Inhabilitación para el ejercicio de funciones o empleos públicos por un periodo de hasta tres años luego de cumplida o conmutada la pena cuando el delito fue cometido con abuso de una posición de acceso a la data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio de un cargo o función públicos.**

b. **Inhabilitación para el ejercicio de la profesión, arte o industria por un periodo de hasta tres años luego de cumplida o conmutada la pena, cuando el delito fue cometido con abuso de una posición de acceso a la data o información reservada o al conocimiento privilegiado de contraseñas en razón del ejercicio privado de la profesión u oficio.**

c. **Inhabilitación para laborar en instituciones o empresas del ramo por un período de hasta tres años luego de cumplida o conmutada la pena, cuando el delito fue cometido con abuso de una posición de acceso a la data o información reservada o al conocimiento privilegiado de contraseñas en razón del desempeño en una institución o empresa privada.**

<u>Artículo 23:</u> Consecuencias accesorias

Se puede imponer la consecuencia accesoria del decomiso prevista en el artículo 102 del Código Penal. En especial, se decomisan los equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualesquiera objetos que fueron utilizados en la comisión de los delitos previstos en la presente Ley. El juez penal puede incautar cautelarmente estos objetos conforme a la normativa penal correspondiente.

Del mismo modo, se pueden aplicar las consecuencias accesorias previstas en el artículo 105 del Código Penal a las personas jurídicas por cuya actividad se realizo o con cuya organización se facilito o encubrió alguno de los delitos previstos en la presente Ley.

<u>Artículo 24:</u> Colaboración eficaz

Puede reducirse la pena hasta por debajo del mínimo legal en el caso de autores y eximirse de la pena en el caso de partícipes que, encontrándose incursos en una investigación a cargo del Ministerio Público o en el desarrollo de un proceso penal por cualquiera de los delitos previstos en la presente Ley, proporcionan información eficaz que permita lo siguiente:

a. **Evitar la continuidad o consumación del delito.**

b. Conocer las circunstancias en las que se cometió el delito e identificar a los autores y partícipes.

La pena del autor se reduce hasta por debajo del mínimo legal y el partícipe quede exento de pena si, durante la investigación a cargo del Ministerio Público o en el desarrollo de un proceso penal en el que estuvieran incursos, restituyen voluntariamente al agraviado la totalidad de los bienes o valores apropiados o entregan una suma equivalente a su valor. Si el delito fue cometido por dos o más autores o dos o más partícipes, la reducción o exención de pena se aplica solamente a quienes realicen la restitución o entrega del valor.

Artículo 25: Codificación de la pornografía infantil

La Policía Nacional del Perú, puede mantener en sus archivos, con la autorización respectiva del Ministerio Público, material de pornografía infantil, en medios de almacenamiento magnético, para fines exclusivos del cumplimiento de su función. Para tal efecto, debe contar con una base de datos debidamente codificada.

Artículo 26: Agente encubierto en el ciberespacio

Con autorización del fiscal, de acuerdo con las circunstancias del caso, se puede emplear el correo electrónico de un detenido por pornografía infantil o por practicar cualquier otro acto ilícito valiéndose de la internet, con el objeto de suplantarlo y obtener más información que ayude a identificar a las demás personas con quienes comete los actos ilícitos mencionados en la presente Ley y el Código Penal, en lo que corresponda.

Artículo 27: Acceso a información de los protocolos de internet

No se encuentra dentro del alcance del secreto de las comunicaciones la información relacionada con la identidad de los titulares de telefonía móvil; los números de registro del cliente, de la línea telefónica y del equipo; el tráfico de llamadas y los números de protocolo de internet (números IP). Por lo tanto, las empresas proveedoras de servicios de telefonía e internet debe proporcionar la información antes señalada conjuntamente con los datos de identificación del titular del servicio que corresponda, a la Policía Nacional del Perú o al Ministerio Público dentro de las cuarenta y ocho horas de recibido el requerimiento, bajo responsabilidad, cuando estas instituciones actúen en el cumplimiento de sus funciones.

CAPÍTULO VIII
DISPOSICIONES PROCESALES

Artículo 28: Intervención y control de las comunicaciones y documentos privados

La facultad otorgada al fiscal para solicitar al juez penal la intervención y control de las comunicaciones, establecida en la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional, también puede ser ejercida en la investigación de los delitos informáticos regulados en la presente Ley. En los lugares en los que haya entrado o entre en vigencia el Nuevo Código Procesal Penal, se aplicaran las reglas de este código para la intervención de las comunicaciones.

<u>Artículo 29:</u> Reserva de la investigación

La investigación que se haga sobre delitos informáticos en la que esté de por medio información cuya difusión pueda generar pánico en sectores sensibles es de carácter reservado, bajo responsabilidad. Queda prohibido a los operadores del sistema penal revelar información o suministrar material incorporados en la investigación a terceras personas o a medios de comunicación social.

DISPOSICIÓN COMPLEMENTARIA MODIFICATORIA

<u>ÚNICA</u>: Modificación de la Ley 27697, Ley que otorga facultad al fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional.

Modificase el artículo 1 de la Ley 27697, modificado por la Ley 28950, Ley contra la trata de personas y el tráfico ilícito de migrantes, y el Decreto Legislativo 991, Decreto Legislativo que modifica la Ley 27697, el cual queda redactado en los términos siguientes:

> **"Artículo 1. Marco y finalidad**
>
> La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.
>
> Sólo puede hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:
>
> a. Secuestro
> b. Trata de personas
> c. Pornografía infantil
> d. Robo agravado
> e. Extorsión
> f. Tráfico ilícito de drogas
> g. Tráfico ilícito de migrantes
> h. Asociación ilícita para delinquir
> i. Delitos contra la humanidad
> j. Atentados contra la seguridad nacional y traición a la patria
> k. Peculado
> l. Corrupción de funcionarios
> m. Terrorismo
> n. Delitos tributarios y aduaneros
> o. Lavado de Activos
> ***p. Delitos Informáticos***
> q. ***<u>-Violación del secreto de las comunicaciones comprendidas en los artículos 161° al 164° del Código Penal.</u>***
> r. Otros delitos, cuando existan suficientes elementos de convicción que permitan prever que el agente forma parte de una organización criminal".

DISPOSICIÓN COMPLEMENTARIA DEROGATORIA

<u>ÚNICA:</u> Derogatoria

Derogan el numeral 3 del segundo párrafo del artículo 186, y los artículos 207-A, 207-B y 207-C del Código Penal.

Sala de la Comisión de Justicia y Derechos Humanos del Congreso de la República, a los seis días del mes de Diciembre de 2011.

ABD/jlcd.