COMISIÓN DE ANTEPROYECTO DE CÓDIGO PENAL 2013

PROPUESTA DE REGULACIÓN
DELITOS INFORMÁTICOS

GUSTAVO BALMACEDA HOYOS

Santiago, 22 de octubre de 2013

I. ARTICULADO

I.1) Primer grupo: delitos contra la intimidad

Artículo A.– Acceso no consentido a sistemas informáticos, apoderamiento de información e interceptación de telecomunicaciones.

El que sin autorización accede a todo o parte de la información o datos personales contenidos en un sistema informático que se encuentren en archivos, correos electrónicos, o en cualquier otro tipo de documento o programa, por medio de la vulneración de medidas de seguridad, interceptación de telecomunicaciones o de cualquier otra señal de comunicación, la permanencia dentro del sistema informático en contra de la voluntad de quien tenga el legítimo derecho de excluirlo, o a través de cualquier otro medio que permita obtener dicha información o datos, será castigado con la pena de xxxx.

Si el acceso se produce con el correlativo apoderamiento de información la pena se agravará a xxxx. La misma pena se aplicará a quien se aprovechase de la información o datos personales conociendo su origen ilícito, y sin haberse tomado parte del acceso y/o apoderamiento de la información o datos.

Artículo B.– Habeas data

El que sin autorización dañe, borre, deteriore, altere o suprima datos reservados de carácter personal o familiar en perjuicio del titular o de un tercero, que se hallen reservados en soportes informáticos, telemáticos o en cualquier otro tipo de archivo o registro público o privado, será castigado con la pena de xxxx.

Si no se realizaren las conductas anteriores pero hay aprovechamiento de los datos conociendo su origen ilícito, la pena se agravará a xxxx.

Artículo C.– Actos preparatorios

El que produzca, venda, obtenga para su utilización, importación o difusión, o posea, programas, dispositivos, códigos de acceso o contraseñas concebidos para la realización de las conductas descritas en los artículos precedentes, incurrirá en la pena de xxxx

Artículo D.- Calificación:

En los casos de los artículos precedentes la pena se agravará a xxxx:

1º Si el delito se cometiere por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros.

2º Si además existiere difusión, revelación, o cesión de la información o datos personales a terceros.

3º Si la víctima fuere menor de 18 años o un incapaz.

4º Si el delito se cometiere con ánimo de lucro.

5º Si el delito se cometiere en el seno de una organización criminal.

I.2) Segundo grupo: delitos contra el patrimonio y el orden socioeconómico

Artículo E.– Fraude informático

El que con ánimo de lucro obtenga para sí mismo o para un tercero, un beneficio económico en perjuicio de otro, a través de cualquier manipulación informática o artificio semejante, será castigado con la pena de xxxx.

En los casos del inciso precedente, serán actos preparatorios punibles que se castigarán con la pena de xxxx la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados para la comisión de fraude informático.

En los casos de los incisos precedentes la pena se agravará a xxxx:

1º Si el monto del perjuicio fuere igual o superior a xxx UTM.

2 º Si el delito se cometiere en el seno de una organización criminal.

Artículo F.– Sabotaje informático

El que sin autorización dañe, borre, altere, suprima, haga inaccesible o realice cualquier conducta semejante sobre datos o el funcionamiento de un sistema informático, será castigado con la pena de xxxx.

En los casos del inciso precedente, serán actos preparatorios punibles que se castigarán con la pena de xxxx la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados para la comisión de sabotaje informático.

En los casos de los incisos precedentes la pena se agravará a xxxx:

1º Si el sabojate informático originare un perjuicio igual o superior a xxx UTM.

2 º Si el delito se cometiere con ánimo de lucro.

3 º Si el delito se cometiere en el seno de una organización criminal.

4 º Si la conducta afectare gravemente los intereses generales o recae sobre instalaciones de telecomunicaciones.

Artículo G.– Infracciones informáticas a la propiedad intelectual

El que reproduzca, plagie, modifique o distribuya, con ánimo de lucro y a través de un sistema informático, una obra literaria, artística, científica y demás creaciones protegidas por la Ley 17.336, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o sus cesionarios, y en perjuicio de éstos, será castigado con la pena de xxxx.

En los casos del inciso precedente, serán actos preparatorios punibles que se castigarán con la pena de xxxx la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados para la comisión de infracciones informáticas a la propiedad intelectual.

En los casos de los incisos precedentes la pena se agravará a xxxx:

1º Si el monto del perjuicio fuere igual o superior a xxx UTM.

2 º Si el delito se cometiere en el seno de una organización criminal.

Artículo H.– Protección de datos de personas jurídicas y de secretos empresariales
El que accediere o se apoderare por cualquier medio de datos, documentos, soportes informáticos o programas reservados de una persona jurídica sin autorización para descubrir un secreto de empresa o con cualquier otro propósito, incurrirá en la pena de xxxx.
La misma pena se aplicará a quien se aproveche de los datos, documentos, soportes informáticos o programas reservados con conocimiento de su origen ilícito, y sin haberse tomado parte del acceso y/o apoderamiento.
En los casos de los incisos precedentes la pena se agravará a xxxx:
1º Si además existiere difusión, revelación, o cesión a terceros.
2º Si el delito se cometiere por quien tuviere legal o contractualmente la obligación de guardar reserva.
3º Si el delito se cometiere con ánimo de lucro.
4º Si el delito se cometiere en el seno de una organización criminal.

I.3) Tercer grupo: delitos contra la fe pública y privada
Artículo I.- Falsedad informática
El que sin autorización introduzca, altere, borre o suprima datos, generando datos no auténticos con la intención de que sean percibidos o utilizados como auténticos, será castigado con la pena de xxxx.
En los casos del inciso precedente, serán actos preparatorios punibles que se castigarán con la pena de xxxx la fabricación, introducción, posesión o facilitación de programas informáticos específicamente destinados para la comisión de falsedad informática.
En los casos de los incisos precedentes la pena se agravará a xxxx:
1º. Si el delito se cometiere con ánimo de lucro.
2º Si el delito se cometiere en el seno de una organización criminal.

I.4) Cuarto grupo: delitos contra la indemnidad sexual

Artículo J.- Child grooming
El que a través de Internet, del teléfono o de cualquier otra tecnología de la información y la comunicación, contactare a un menor de 14 años y proponga concertar un encuentro a fin de cometer un atentado sexual, siempre que tal propuesta se acompañe con actos materiales de acercamiento, será castigado con la pena de xxxx. La pena se agravará a xxxx cuando el acercamiento se obtenga por medio de coacción, intimidación o engaño.

Artículo K.- Corrupción de menores (pornografía infantil)
Será castigado con la pena de xxxx, al que produzca, distribuya, venda, exhiba o almacene para estos fines utilizando un sistema informático o cualquier otro medio semejante, material pornográfico o que contenga actos de significación sexual realizados con menores de edad e incapaces.
Quien facilite la realización de las conductas anteriormente descritas será castigado con una pena de xxxx. Igual pena se aplicará cuando el material pornográfico o con actos de significación sexual sea realizado por una persona representando a un menor.

Artículo L.- Circunstancias agravantes

La pena se agravará a xxxx cuando concurra cualquiera de las siguientes circunstancias:

a) Cuando se utilice a un menor de 14 años.

b) Cuando los hechos revistan un carácter degradante o vejatorio.

c) Cuando los hechos revistan especial gravedad, atendiendo el valor económico del material pornográfico.

d) Cuando el material pornográfico represente a niños o incapaces que son víctimas de violencia física o sexual.

e) Cuando el material pornográfico sea producido, distribuido, vendido o exhibido en el marco de una organización criminal.

f) Cuando se usa fuerza o intimidación.

g) Cuando se abusa de la enajenación o trastorno mental de la víctima o de una anomalía o perturbación mental, aun transitoria, de la víctima, que por su menor entidad no sea constitutiva de enajenación o trastorno.

h) Cuando se abusa de una relación de dependencia de la víctima.

i) Cuando se abuse del grave desamparo en que se encuentra la víctima.

j) Cuando se engaña a la víctima abusando de su inexperiencia o ignorancia sexual.

Artículo M. Posesión de material pornográfico de menores

El que posea material pornográfico en un sistema informático, medio de almacenamiento o cualquier otro medio semejante en cuya elaboración se hayan utilizado menores de edad o incapaces, será castigado con la pena de xxxx.

Artículo N.- Guarda o tutela

Será castigado con la pena de xxxx, el que tuviere bajo su potestad, tutela, guarda o cuidado a un menor de edad o incapaz y que, con conocimiento de su estado de prostitución o corrupción a través de medios informáticos, no acuda a la autoridad competente para impedir la continuación de tal estado.

Artículo O.- Menor o incapaz como destinatario de material pornográfico

El que por cualquier medio directo vendiere, difundiere o exhibiere material pornográfico entre menores de edad o incapaces, será castigado con la pena de xxxxx

II. FUNDAMENTACIÓN GENERAL

La evolución de las tecnologías de la información y las comunicaciones (en adelante, TIC) y de la revolución informática han producido, paralelamente, transformaciones criminológicas que fueron dejando a ciertas figuras delictivas obsoletas. Así, la creación y desarrollo durante los últimos años de la *Internet* y, en general, de las TIC han traído consigo cambios sociales y culturales que no son ajenos al mundo del Derecho (especialmente, al Derecho penal); por el contrario, en los últimos años se han elaborado instrumentos legales tanto a nivel nacional como internacional para responder a las necesidades de salvaguardar ciertos intereses y bienes jurídicos que se han visto afectados por esta nueva ola informática (en especial, el *Convenio sobre cibercriminalidad* suscrito en el seno del Consejo de Europa, celebrado en Budapest el 23 de noviembre de 2001, el que se ha tenido presente en esta propuesta).

Lo anterior demuestra que la revolución informática y, con ella, la *Internet* y las TIC hacen necesaria una reformulación de las tradicionales categorías criminológicas debido a que con el espacio digital y las nuevas formas de tratamiento de la información hay un cambio del marco espacio-temporal en que se cometían los delitos tradicionales, por ello, en ciertos casos resulta forzoso ajustar determinadas modalidades de conductas que se realizan en otro campo diferente al físico a las teorías criminológicas tradicionales. Así las cosas, consecuencias tales como la modificación y ampliación del ámbito de oportunidad criminal, el aumento el número de agresores y de potenciales víctimas con características propias, el rol que éstos cumplen en la ejecución del delito, el acrecentamiento de los efectos multiplicadores del delito, los nuevos tipos de comportamientos que afectan de forma diferente a los bienes jurídicos tradicionales y la aparición de intereses difusos que llegaron a tener contenido con las TIC, entre otros, deben ser tenidas en cuenta a la hora de establecer una categoría criminológica sobre la *delincuencia informática* debido a la inaplicabilidad de una cantidad no despreciable de normas jurídicas actualmente vigentes.

En concreto, la realidad criminológica que motivó en Chile la dictación de la Ley 19.223 es muy diferente a la actual. Piénsese, por ejemplo, que ni siquiera se había masificado la *Internet* en nuestro país al momento de su discusión parlamentaria. Ello se demuestra, también, a partir de la propia denominación que se le ha otorgado a ésta categoría de delitos. Tradicionalmente, se ha utilizado el término de "delito informático" para hacer referencia a aquellas figuras delictivas que emplean de una u otra forma medios informáticos. Sin embargo, esta denominación no resulta apta para agrupar a todas las conductas ilícitas cometidas con injerencia de las TIC, pues no permite insertar dentro de una misma categoría tanto a aquellos comportamientos delictivos "nuevos" realizados a través de procesos electrónicos como a los delitos "tradicionales" que han encontrado en la revolución tecnológica un campo propicio para su comisión y expansión. Adicionalmente, no permite diferenciar con claridad aquellos delitos que emplean el medio informático como vehículo para su comisión, de aquellos en donde los sistemas informáticos o la información contenida en éstos son el objeto mismo del ataque.

Al hablar de "delito informático" como categoría dogmática, en nuestra opinión, se deja de lado que existe una pluralidad de delitos y de comportamientos cuya única característica en

común es el uso de las TIC, por lo cual, cada uno de ellos posee diferentes problemas "dogmáticos" al emplear diversas modalidades de comisión y afectar diferentes tipos de bienes jurídicos pero, no obstante, convergen al poseer una misma problemática de riesgo y al afectar, al parecer, intereses sociales similares. En este sentido, el término "delito" hace alusión a comportamientos tipificados por el legislador como tales, por lo cual, al usar el vocablo referido se desconoce que en las TIC son múltiples las modalidades de comportamientos que contravienen los intereses sociales sin ser delitos en sentido estricto y que, además, se encuentran en constante modificación y evolución, lo que hace imposible la sistematización de las conductas por medio de un catálogo "exhaustivo" (esto es, "completo y acabado") en la ley penal que se adecue a las necesidades sociales. En la práctica, entonces, la exigencia de una legislación que categorice una conducta como delito, hace que los hechos que vulneran o violan intereses esenciales para la existencia del sistema y que aún no han sido tipificados queden al margen de acción del Derecho penal a pesar de la necesidad de protección jurídica.

En consecuencia, es necesario cambiar la categorización de "delitos informáticos" para adoptar un término criminológico que sea amplio y funcional, reconocedor del "fenómeno", como podría ser, por ejemplo, la voz "*cibercrimen*", que trae como beneficio el poder permitir evidenciar que el elemento común a los delitos que lo conforman son las "TIC" como medio o como objeto de comisión delictiva, y permite abarcar al "*ciberespacio*" o *espacio virtual* como factor de incidencia criminológica en el que la interacción entre el mundo físico y el cibernético modifica algunos de los elementos del delito, y se logra englobar diversas tipologías de comportamientos. Asimismo, ésta ha sido también la opción escogida por el legislador internacional en el Convenio sobre cibercriminalidad. En concordancia con ello (y para no afectarse, por cierto, el principio de legalidad, ni tampoco abogando por una "expansión") se tiene como propósito para la tipificación de estas conductas *identificar grupos de problemas* que sean subsumibles a través de la creación de "tipos de equivalencia" (es decir, se trata de la búsqueda de la creación propiamente tal de nuevos tipos penales, o que perfeccionen a los ya existentes corrigiendo las carencias detectadas en aquellos). Al no tenerse presente al momento de la siguiente propuesta la descripción típica de algunos delitos, por ejemplo, los referidos a la indemnidad sexual, en esos supuestos se proponen como conductas típicas únicamente lo referido en específico a las TIC. Algo similar se puede decir a propósito de las normas adecuatorias de carácter procesal, puesto que el profesor informante no es experto en esa materia. Por ello, sobre este último aspecto la presente propuesta se limita a exponer las recomendaciones consensuadas a nivel internacional.

Es menester señalar que al intentar aglomerar bajo una sola rúbrica tanto aquellas conductas que puedan ser incardinadas dentro del catálogo de delitos existente, como en los comportamientos que aun sin ser delitos en estricto sentido son conductas reprochables o causantes de graves perjuicios sociales, que pueden llegar ser objeto de sanción penal; y al aceptar que no hay un delito informático como tal, se está dejando a un lado como objeto de protección el concepto de bienes jurídicos. En este sentido, la categoría penal *sub examine* no se encamina a salvaguardar bienes jurídicos asignados específicamente a ésta, es decir, no existe en nuestra opinión un "único" bien jurídico informático, sino intereses colectivos difusos con una misma problemática de riesgo que no alcanzan a ser bienes jurídicos porque muchas de las modalidades de comportamientos afectan intereses que no se han cristalizado en bienes

jurídicos tutelados por el Derecho penal y porque una conducta dañina puede afectar diversos bienes jurídicos. Por ello es necesario realizar un análisis tipológico amplio donde se acepte la delincuencia informática como categoría criminológica que abarque todos los comportamientos que se presentan en el ciberespacio aunque no se encuentren tipificados como delitos. En otras palabras, en la delincuencia informática existe un interés social esencial de por medio; que por la diversidad y heterogeneidad de conductas que pretenden ser cubiertas, se protegen intereses colectivos y no necesariamente bienes jurídicos particulares, lo cual va en la misma dirección de corrientes doctrinarias que están avalando la tutela intereses difusos, colectivos o macrosociales por medio del Derecho penal.

Lo anterior se debe a lo siguiente: existen conductas que aun sin ser delito en sentido estricto constituyen pasos previos que en algunos casos podrán ser reputados como tentativas delictivas y en otros no. Es lo que sucede, por ejemplo, con el *spam*, o con algunas infecciones de *malware* que no causando ningún daño se realizan, en última instancia, como pasos necesarios para el posterior acceso ilícito al sistema o la futura defraudación.

En segundo lugar, se trata de un fenómeno transnacional regulado de forma distinta por muchos Estados que no siempre seleccionan las mismas conductas para su sanción penal, por lo que resulta más adecuada una visión omnicomprensiva de los *ciberataques* que los incluya a todos, sean o no penados. Tercero, y desde una perspectiva criminológica, nos interesa el *cibercrimen* como una categoría amplia en aras de la prevención del mismo. Y, finalmente, muchos de los intereses no alcanzan al nivel de bienes jurídicos tutelados por el legislador penal debido al constante cambio y evolución de las modalidades de comportamiento que afectan tanto antiguos bienes jurídicos como nuevos intereses difusos que salieron a flote cuando surgió la criminalidad en las TIC.

Teniendo en cuenta lo anterior, y dejando sentado que no se busca un capítulo particular dentro del Código Penal dedicado al *cibercrimen,* ya que se toma como categoría criminológica amplia –sentido tipológico– que sirva para incluir todas las modalidades de comportamientos, la ubicación de la conducta penalmente reprochable se realizará de forma difusa según el bien jurídico que se lesiona o pone en peligro de tal forma que se admitan tipos abiertos que sean coherentes con el constante cambio y evolución de las conductas lesivas. De esta manera, nos parece que se evitarían lagunas de punibilidad.

Adicionalmente, sólo para efectos pedagógicos a efectos de poder entender los grupos de problemas que genera la *cibercriminalidad*, se usará la clasificación dogmática de "ciberataques puros", en los cuales se agrupan aquellos comportamientos nuevos que se caracterizan por dirigirse contra nuevos bienes o intereses jurídicos y, por tanto, requieren establecer nuevas estrategias político-criminales a través de "tipos de equivalencia"; y los "ciberataques réplicas", es decir, aquellos delitos tradicionales que se realizan por medio de las TIC y el *ciberespacio* aprovechando las nuevas oportunidades delictivas, para lo cual serán subsumibles en los tipos tradicionales: aquí se requerirá una modificación de los tipos penales existentes si se alteran elementos del delito, si no hay tal alteración la conducta se puede incorporar dentro de los tipos delictivos clásicos (por ejemplo, hipótesis en que se agrava el tipo). Dentro de esta clasificación se puede identificar, a su vez, cuándo los sistemas informáticos pueden ser usados como medio para realizar la conducta o cuándo son el objeto de afectación, sin embargo, no

optamos derechamente por esta diferenciación porque consideramos que la clasificación propuesta permite comprender mejor la realidad criminológica del fenómeno y optar por medidas preventivas comunes según el tipo de comportamiento.

Finalmente, a efectos de poder esclarecer la interpretación, se asume la terminología del Convenio sobre cibercriminalidad en su artículo primero en el siguiente sentido:

Por "*sistema informático*" se designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;

Por "*datos*" se comprenden toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función; o, todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

III. FUNDAMENTACIÓN ESPECIAL

Artículo A.– Acceso no consentido a sistemas informáticos, apoderamiento de información e interceptación de telecomunicaciones.

COMENTARIO:

La protección de los sistemas informáticos en la actualidad resulta ser de gran importancia debido a que a partir de dicha protección depende el resguardo de muchos bienes jurídicos que se ejercen y proyectan dentro de éstos, de ahí la necesidad de penalizar el acceso no consentido a sistemas informáticos. Así, la conducta típica del inciso primero del presente artículo recae sobre la información o datos personales contenidos en sistemas informáticos que se encuentren en cualquier tipo de documento o programa. Al incluir la expresión "o en cualquier otro tipo de documento o programa" se evidencia la necesidad de extender el objeto material del delito debido a la constante evolución de los sistemas de almacenamiento de datos. Entonces, lo importante es la determinación de si la información o datos contenidos en éstos son de carácter "personal", pues es ahí en donde se encuentra delimitado el objeto de protección del artículo, para lo cual aceptamos que es la voluntad del sujeto con la existencia de un interés relevante jurídicamente el criterio que debe ser analizado caso a caso para fijar su calidad de "personal" por constituir, a fin de cuentas, información y datos que proyectan la intimidad del sujeto.

Adicionalmente, se establece como modalidades de comisión, primero, la "vulneración de medidas de seguridad" que abarca, entre otros, al llamado *Hacking*, conducta en la que se utilizan técnicas para acceder "sin autorización" a sistemas informáticos. Se tipifica expresamente la conducta "sin autorización" y no "contra la autorización", porque se trata de

una modalidad comitiva más amplia, lo que político-criminalmente se estima razonable por la entidad de los bienes jurídicos que se encuentran en juego –el mismo razonamiento es válido para todas aquellas conductas que se tipifican de la misma manera a lo largo de la presente propuesta–.

La protección de la intimidad dentro de los sistemas informáticos depende, en buena medida, de la propia víctima, por ello, la existencia de barreras que ésta constituye sobre la información y los datos permite dilucidar el ánimo de otorgarles carácter de "reservados". Por esta razón, una introducción a un sistema "sin autorización" debe ser considerada como delito por violentar la intimidad, bastando para su consumación la vulneración de medidas de seguridad, como por ejemplo, de las claves de acceso, independientemente del contenido real de la información.

En segundo lugar, se menciona la "interceptación de telecomunicaciones", haciendo referencia a la intromisión sin autorización durante el proceso de transmisión y recepción de señales de tecnologías, como lo son por ejemplo el teléfono y telefonía móvil, y en la comunicación de datos y redes informáticas como *Internet* y, además, estableciendo una clausula "amplia" en donde se acepta la posibilidad de interceptación de otras señales de comunicación que puedan crearse gracias al avance tecnológico, de tal forma que el delito se consuma con la efectiva interceptación, independientemente de lo que se descubra.

Finalmente, se hace referencia a "la permanencia dentro del sistema informático en contra de la voluntad de quien tenga el legítimo derecho de excluirlo" que envuelve los eventos en que un sujeto accedió autorizado legítimamente al sistema informático pero continúa en su interior a pesar de revocársele el permiso. Sin embargo, las modalidades señaladas anteriormente sirven como asientos o ejemplos de modalidades comisivas y se acepta la posibilidad de que se generen otras formas de conductas ilícitas, lo cual se puede deducir de la disposición, "o a través de cualquier otro medio que permita obtener dicha información o datos".

Por otra parte, el inciso segundo se refiere al *apoderamiento*. La diferencia entre el "acceso" del inciso primero y el "apoderamiento" radica en que este último exige poseer la información o los datos, es decir, realizar conductas como, por ejemplo, copiar archivos; y, por su parte, el *acceso* consiste en una mera intromisión o interceptación sin desplazamiento de la información y no implica *aprehensión* sino "conocimiento no autorizado" sin alterar, copiar, mover o desplazar el soporte original. Por ello se realiza una diferenciación entre ambas conductas y se propone una pena más grave para el *apoderamiento* por revestir un mayor grado de vulneración de los bienes jurídicos protegidos. Finalmente, se castiga con la misma pena a quien "se aprovechase de la información o datos personales conociendo su origen ilícito, y sin haberse tomado parte del acceso y/o apoderamiento de la información o datos", pues consideramos que la gravedad de la conducta es mayor que el simple acceso y puede equipararse al apoderamiento.

Para concluir, debemos señalar que no se exige un fin o elemento tendencial subjetivo específico como lo hace, por ejemplo, el CP español en su artículo 197.1 que indica que la conducta debe estar dirigida con la intención de descubrir secretos o vulnerar la intimidad de

otro. En este sentido, el Convenio sobre cibercriminalidad en su artículo 2 establece que los Estados Partes "podrán" exigir que la infracción sea cometida con la intención de obtener los datos informáticos o con otra intención delictiva, por lo cual el legislador facultativamente puede omitir dicha exigencia. Conforme a lo anterior, excluimos un ánimo especial como requisito para la configuración del delito, debido a que se restringirían las conductas punibles y aumentarían los problemas de carácter probatorio que ya son propios de este tipo de delitos por circunstancias, como por ejemplo, derivadas del anonimato que confiere *Internet*.

Artículo B.– Habeas data

COMENTARIO:

El presente artículo busca asegurar el derecho al *habeas data* sobre aquellos datos personales que se encuentren automatizados dentro de un sistema informático. Como parte de la protección de la facultad que poseen los individuos de conocer, actualizar, excluir y rectificar la información que se contenga en banco de datos, tanto públicos como privados, es decir, del poder de control de la información personal que terceros puedan poseer, es menester tipificar como ilícitos penales aquellas conductas realizadas contra los datos digitalizados almacenados, pues es innegable su vulnerabilidad a raíz de que el formato, almacenamiento y transmisión aumenta considerablemente el perímetro de daño.

Para la configuración del delito debe haber concurrencia, por una parte, de la falta de autorización, lo cual indica que el consentimiento determinará la vulneración o no del derecho al *habeas data*. Por otra parte, se exige el ánimo de perjudicar al titular o a un tercero, es decir, se requiere un dolo que puede ser directo o eventual en aquellos casos en que el sujeto asuma como posible que cualquier persona pueda ser perjudicada como consecuencia de la utilización de los datos. De esta manera, la expresión "en perjuicio del titular o un tercero" denota que basta con que la finalidad del autor se encamine, directa o indirectamente, a generar un perjuicio para un tercero.

Finalmente, en el inciso final se castiga a quien se aprovecha de la información con una pena más grave configurándose un delito autónomo que busca evitar el uso de la información por parte de terceros.

Artículo C.– Actos preparatorios

COMENTARIO:

En este caso se señalan los actos preparatorios punibles que de no estar expresamente sancionados serían actos impunes. Así, se debería castigar con una pena menor la puesta en peligro abstracto que supone la realización de conductas iniciales necesarias para cometer las infracciones informáticas contra la intimidad, lo cual se estima necesario debido a que es político-criminalmente razonable reforzar la protección penal por el aumento de la vulnerabilidad de los bienes jurídicos por aspectos propios que caracterizan a los crímenes

realizados en los nuevos espacios informáticos como lo son la deslocalización, la libertad de los usuarios, la revolución permanente de las conductas comisivas, el anonimato que confiere el uso de terminales informáticas, entre otros.

Esta incriminación, entonces, se explica por la influencia que contemporáneamente han alcanzado los programas informáticos en el tráfico económico en general, y a que de esta manera se le debe conceder una protección específica y robustecida al sistema.

Artículo D.- Calificación.

COMENTARIO:

En este artículo se realiza una sistematización de agravantes que consideramos relevante tener en cuenta al momento de incriminar la conducta por aportar un especial desvalor o reproche de la conducta. Así, los delitos contra la intimidad se comportan como un tipo penal compuesto, que requiere la previa comisión de uno de los tipos básicos.

La agravante contemplada en el numeral 1° se explica por el deber de cuidado que tiene el sujeto activo sobre la información que custodia y por el aprovechamiento de las facilidades que para la comisión del delito implican los vínculos, lo que significa una mayor posibilidad en la ejecución del mismo.

Respecto al numeral 2°, debemos decir que los delitos antes descritos están concebidos de tal forma que no es relevante si efectivamente se realiza un descubrimiento de información o datos de carácter personal o si hubo un perjuicio real para la víctima o para un tercero como se explicó en líneas anteriores. Tal descubrimiento de la intimidad del sujeto sólo será relevante si se difunde, revela o cede, constituyendo en este caso un tipo agravado. Ahora bien, la diferencia entre difusión y revelación radica en que en la primera va implícito una idea de publicidad de la información.

Por otra parte, la agravante del numeral 3º se justifica porque se estima que es necesario realizar una protección reforzada sobre los menores de edad e incapaces, pues debido a su vulnerabilidad debe fortalecerse la protección del derecho a la intimidad con una mayor incriminación de conductas que los afecte.

A su vez, el numeral 4° contempla como tipo agravado los fines lucrativos que presiden el atentado a la intimidad. Se utiliza esta técnica de tipificación debido a que, por una parte, exigir ánimo de lucro para configurar el delito implicaría darle matices patrimoniales a la tutela de un bien jurídico estrictamente personal, por otro lado, la estructuración de delitos fundamentados en elementos exclusivamente anímicos o subjetivos resulta ser contraproducente por aspectos procesales, como por ejemplo, los problemas probatorios que implican. Por ello se optó por establecer el ánimo de lucro no como elemento anímico especial que debe estar presente en la realización de la conducta, sino como un agravante que requiere la realización del tipo básico.

Finalmente, la agravante del numeral 5º se justifica porque las características propias de los nuevos espacios en donde se desarrollan las comunicaciones y el tratamiento de la información digitalizada tales como el *ciberespacio* y, en general, las tecnologías de la información y la comunicación, así como la transnacionalidad de la red, su universalización y el anonimato que otorga, se convierte en un campo delictivo propicio para el desarrollo de actividades de organizaciones criminales, lo que hace necesario agravar las conductas que se desarrollen en ese marco.

Artículo E.– Fraude informático

COMENTARIO:

El desarrollo de actividades económicas, financieras y comerciales aprovechando las ventajas que genera el uso de sistemas informáticos ha estado acompañado del aumento de delincuencia económica a través de los medios informáticos que se valen de la escasa protección contra los ataques, por ejemplo, utilizando programas que determinan la transferencia de fondos para realizar apropiaciones patrimoniales inmateriales. Por ello se requiere una protección a nivel penal de tal forma que se salvaguarde el tráfico económico.

Hay que subrayar que se utiliza la voz "fraude" y no "estafa", con el propósito de poderse incriminar aquí, no solamente una disposición patrimonial perjudicial "microsocial" que se produzca producto de una manipulación informática o artificio semejante, o sea, una "estafa" que se produzca o genere de la manera expuesta, sino también la generación de perjuicios económicos "macrosociales" –delitos económicos o contra el orden socioeconómico– que se puedan producir de la misma forma. Por ejemplo, una defraudación a la seguridad social, a la hacienda pública, o un delito aduanero.

El presente artículo requiere un elemento intencional concretado en el ánimo de lucro, entendido como "ánimo de enriquecimiento" y no como un mero "aprovechamiento", y la realización de manipulaciones informáticas o artificios semejantes para obtener beneficios económicos, lo cual significa que el sujeto activo debe realizar conductas tendientes a generar por parte de un sistema informático una merma patrimonial en perjuicio de "otro". Se subraya esta voz y no "tercero", para destacar su carácter amplio y para evitar discusiones estériles, por ejemplo, si se tiene o no personalidad jurídica, etc.

Con lo anterior se busca incriminar conductas que vayan más allá de la estafa clásica o tradicional, pues en este caso según la mayoría de la doctrina se requeriría engaño y error para lograr la propia colaboración de la víctima, lo que no abarcaría la manipulación o alteración informática de los computadores sin un correlativo engaño que muchas veces no se presentaría debido a la inexistencia de un contacto personal y directo entre el sujeto activo y pasivo.

En este orden de ideas, la manipulación informática consiste en "cualquier" alteración o modificación de los datos, que puede consistir en supresión, introducción de nuevos datos falsos, modificación dentro del programa, etc., pero acompañado del correlativo ánimo de

lucro y obtención de un beneficio económico para sí mismo o para un tercero, junto a la realización del acto de disposición y perjuicio patrimonial de "otro" que implicaría el cambio de titularidad del elemento patrimonial a través de operaciones informáticas. Lo anterior diferencia esta figura del delito de la denominada "falsedad informática". De otro lado, la expresión "artificio semejante" se incluye para evitar lagunas de punibilidad, con el propósito de intentar hacer frente a lo vertiginoso del avance de las TIC y realidad criminológica frente a este tipo de ilícitos.

En el inciso segundo se incriminan actos preparatorios, a los cuales se los eleva a la categoría de "delitos autónomos" o "formas de participación intentada impropia". Con el propósito de que no se infrinja el principio de proporcionalidad por la imposición de una pena idéntica a la del delito consumado a que se refieren y, asimismo, para que no supongan una vulneración del principio de intervención mínima, porque vienen a castigar comportamientos muy alejados todavía de la efectiva puesta en peligro del bien jurídico, se propone la imposición de una pena menor a las conductas típicas del inciso primero. Aquí nos encontramos frente a un "tipo mixto alternativo", pues se impone una pena "única" por la ejecución de uno de los comportamientos descritos o por todos. Por ello, no interesa que el autor realice una o todas las acciones descritas en la norma. Los comportamientos de fabricación, introducción, posesión o facilitación, por su parte, pretenden comprender todas las hipótesis imaginables vinculadas con la creación de programas informáticos, con el objeto de castigarlas de un modo exhaustivo.

Finalmente, en el último inciso se incluyen agravantes que estimamos político-criminalmente coherentes por aportar un especial desvalor o reproche de la conducta. La determinación del monto del perjuicio "valorable" como una decisión de gravedad, va a depender del criterio de proporcionalidad escogido por la comisión de Anteproyecto de Código Penal al momento de determinar la regulación de la pena en los delitos contra el patrimonio y el orden socioeconómico. Sobre la comisión del delito en el seno de una organización criminal nos remitimos a lo dicho a propósito de los delitos contra la intimidad.

Artículo F.– Sabotaje informático

COMENTARIO:

En el presente artículo se incriminan las conductas bajo la rúbrica de "sabotaje informático" y no meros "daños informáticos", para incluir diferentes comportamientos y poder así castigar la imposibilidad del uso del sistema informático, que muchas veces se produce por actos que van más allá del daño. De esta manera, se puede incluir como objeto material el "sistema informático", cuya inclusión expresa extiende la garantía penal no sólo a los elementos materiales del *Hardware* que permitan el funcionamiento del sistema operativo, sino también a los "inmateriales", es decir, los elementos lógicos que permiten su funcionamiento y las unidades de almacenamiento de la información, de tal forma que la protección abarca a datos y documentos electrónicos que permitan el fruncimiento y el desarrollo de las prestaciones informáticas. En este orden de ideas, los *datos* son entendidos como la información

introducida, almacenada o tratada por el titular y programas que permiten al sistema desarrollar determinadas funciones; y, los documentos electrónicos, por su parte, son soportes digitales de ideas o informaciones configurados "digitalmente".

Respecto a las conductas típicas, se incrimina el "daño", que implica el menoscabo, detrimento, perjuicio o inutilización de los elementos informáticos; el "borrado", que consiste en eliminar datos, archivos, ficheros, programas o documentos electrónicos de su suporte digital o del sistema en que se encontraban gravados; el "alterar", entendido como la modificación en todo o parte del contenido y los elementos del sistema informático; el "suprimir", que debe ser entendido como la realización de conductas que imposibiliten la utilización de funciones sin necesidad de borrarlas o eliminarlas del sistema; y, por último, "hacer inaccesible", que se presenta cuando se impide el acceso, la consulta o el uso de elementos de un sistema informático. La inclusión de la cláusula "o conductas similares" dilucida que lo importante es la "dañosidad", es decir, la afectación de la integridad o funcionamiento del sistema informático, de tal forma que las conductas descritas anteriormente tienen una función meramente enunciativa, con el propósito de evitar lagunas de punibilidad.

Ahora bien, la diferencia con el *acceso no consentido* a sistemas informáticos radica en que en éste debe haber un acceso o apoderamiento de información personal que no requiere un "daño" del sistema informático; y, por otra parte, el *sabotaje informático* lleva implícito un perjuicio económico. Lo anterior es sin perjuicio de que ambos delitos sean compatibles y pueda llegar a presentarse un concurso medial.

Adicionalmente, y siguiendo el esquema planteado a lo largo de la propuesta, la regulación se complementa con un delito de peligro abstracto que consiste en los actos preparatorios que merecen penalizarse con un castigo menor. Sobre los demás aspectos que digan relación con esto, nos remitimos a lo dicho a propósito del fraude informático.

Por último, con respecto a las hipótesis que agravan la conducta, vale la pena hacer referencia al *ánimo de lucro*, ya que el hecho de establecerse como agravante y no en el delito base implica que el delito se configura sin exigirse una motivación especial y que la comprobación de dicha motivación solo es necesario para aumentar la pena, no obstante ser necesario el perjuicio patrimonial para el sujeto pasivo. Por otra parte, el numeral 5 hace referencia al dolo específico de alterar el servicio público, para lo cual deben analizarse las circunstancias que rodean la conducta, la función que cumple el objeto dañado y si recae sobre centros generales de distribución de comunicación.

Artículo G.– Infracciones informáticas a la propiedad intelectual

COMENTARIO:

Se busca proteger el derecho moral del autor, es decir, el derecho de control del autor sobre la obra que implica el reconocimiento de la paternidad y a decidir sobre su integridad, y derechos patrimoniales relativos a la explotación y distribución que contemplan los rendimientos económicos derivados de la comercialización, la reproducción, distribución, comunicación pública y transformación de la obra. De esta forma, para encontrar coherencia entre el ordenamiento jurídico se hace referencia a la Ley 17.336 sobre propiedad intelectual, de tal forma que la interpretación del presente artículo debe hacerse conforme a los conceptos que en ella se establece para determinar, por una parte, el objeto material del delito, y por otra, los sujetos pasivos de la conducta.

Por otra parte, se describen diferentes conductas típicas: la *reproducción* consiste en la realización de una o más copias de la obra o de una parte de ella en cualquier formato material que debe ser analizado desde la perspectiva de los elementos cuantitativos de la reproducción, pues sólo serían ilícitos penales la unión entre la multicopia con ánimo de lucro; el *plagio* consiste en la copia de todo o parte sustancial de obras ajenas, dándolas como propias; la *modificación* consiste en alterar la obra original que viola su integridad; y, la *distribución* consiste en la puesta a disposición del público del original o copias de la obra para su venta, alquiler, préstamo o de cualquier otra forma.

Adicionalmente, se introduce un elemento subjetivo del injusto concretado en el *aprovechamiento* patrimonial por el sujeto activo. No es preciso el efectivo daño patrimonial sino que se evidencie la intención de obtener un beneficio patrimonial con la realización de las conductas descritas. Asimismo, se establece que la conducta debe ser *sin autorización* y en *perjuicio* de los titulares de los correspondientes derechos de propiedad intelectual o sus cesionarios, lo cual indica que basta un dolo eventual, es decir, solamente es necesario que el sujeto conozca y acepte las consecuencias perjudiciales de la conducta.

Posteriormente, se señalan los *actos preparatorios punibles* para otorgar mayor protección a la propiedad intelectual, pues de no estar expresamente sancionadas serían actos impunes. Así, se castiga con una pena menor la puesta en peligro abstracto que supone la realización de conductas iniciales necesarias para realizar infracciones informáticas a la propiedad intelectual. Sobre lo demás, nos remitimos a manifestado a propósito del fraude informático.

Finalmente, se establecen eventos que agravarán la pena siguiendo un criterio patrimonial respecto del daño e incriminando las conductas realizadas en el marco de una organización criminal, elemento que se estima de vital importancia, puesto que permitiría prevenir el tráfico internacional de ejemplares de obras.

Artículo H.– Protección de datos de personas jurídicas y de secretos empresariales

COMENTARIO:

En este artículo se integra tanto la protección genérica para los datos de las personas jurídicas en el marco del derecho a la intimidad como la protección específica de los secretos empresariales que en algunas legislaciones, v.gr. la española, se encuentran disipados en apartados diferentes. Consideramos que no es necesaria dicha diferenciación, porque tipificar los datos de las personas jurídicas como parte del derecho a la intimidad implicaría entrar en discusiones sobre la posibilidad de que entes colectivos puedan ser titulares de éste derecho. Adicionalmente, el hecho de descubrir datos, documentos, soportes informáticos, etc., "con cualquier finalidad", incluyendo la revelación de secretos de empresa, se estima suficiente para la protección del bien jurídico que se pretende tutelar, pues los secretos empresariales son, a fin de cuentas, *datos de las personas jurídicas*, entonces, establecer dos preceptos diferentes acarrearía, en nuestro concepto, problemas sobre el ámbito de aplicación.

El verbo rector constituido por *acceder o apoderarse* está seguido por la indicación de que puede ser realizado por cualquier modalidad comisiva, de tal forma que no se restringe a una sola clase de conducta típica. Por otra parte, es menester recalcar la importancia de que los datos, documentos, soportes informáticos o programas tengan el carácter de "reservados", pues sólo respecto de éstos recae la protección penal, circunstancia que depende del titular del bien jurídico y que, en caso de no existir una declaración expresa, se puede deducir del interés de confidencialidad o exclusividad que objetivamente se desprende de la naturaleza de la información (por ejemplo, movimientos bancarios o procedimientos industriales).

Asimismo, en cuanto al elemento subjetivo del injusto, se exige que el fin sea *descubrir un secreto de empresa o cualquier otro*, de modo que se protejan tanto aquellos documentos que contengan secretos de empresa como otro tipo de datos reservados. Así, no es necesario su "efectivo" descubrimiento, sino que basta con el mero *acceso o apoderamiento*. En el caso contrario, quedarían impunes las conductas de mero acceso o apoderamiento sin dicho ánimo, el cual debe estar presente al momento de realizar la conducta.

Por otra parte, se castiga al *aprovechamiento*, cuyo objetivo consiste en impedir el tráfico de información confidencial y secretos de empresa por terceros ajenos a la conducta de acceso o apoderamiento y, finalmente, se establecen las causas que agravarían la pena siguiendo los criterios que se expusieron con anterioridad, adecuándolos a la conducta descrita y agregando la agravante de "quien tuviere legal o contractualmente la obligación de guardar reserva" que se fundamenta en la relación de confianza y el deber de cuidado que poseen los sujetos que tienen acceso a información reservada.

Artículo I.- Falsedad informática

COMENTARIO:

El tipo básico que castiga las falsedades realizadas a través de sistemas informáticos reconoce que las falsedades documentales desde antes penalizadas ahora pueden cometerse a través de procedimientos informáticos. Así, puede concebirse como un delito con una doble función, ya que, además de garantizar la seguridad de los documentos como bien jurídico autónomo que requiere protección propia, busca prevenir la realización de futuras conductas lesivas, pues la generación de datos no auténticos puede concebirse como pasos previos para la futura realización de estafas, por ejemplo.

De esto se deriva la importancia del inciso segundo que castiga actos preparatorios que en sí mismos resultan potencialmente peligrosos para la indemnidad del bien jurídico protegido y por ello se necesita incorporar un precepto específico para anticipar el castigo a determinados actos previos a la ejecución, que de otro modo habrían de resultar impunes por no hacer parte de una falsedad propiamente tal. Adicionalmente, un documento digital resulta, inicialmente, mucho más fácil de falsificar que un documento en soporte papel, por ello se requiere una protección reforzada que abarque pasos previos a la comisión del delito. Así, si solamente se tiene la mera tenencia de instrumentos, la pena será menor, pero la tenencia correlativa con la falsificación implica una mayor pena.

Artículo J.- Child grooming

COMENTARIO:

La propuesta castiga el contacto con los menores a través de cualquier tecnología de la información y la comunicación con la finalidad de cometer abusos o agresiones sexuales. Se trata de un tipo que castiga actos preparatorios que resulta necesario por la dimensión especial que adquiere el bien jurídico, por el mayor contenido de injusto y por la implicancia de la involucración de menores de edad en contextos sexuales sin consentimiento para la formación de la personalidad y la sexualidad.

De todas formas, se recomienda incriminar la presente conducta en los tipos generales que digan relación con los atentados contra la indemnidad sexual.

Artículo K.- Corrupción de menores (pornografía infantil)

COMENTARIO:

Sobre esto parece indispensable consultar la propuesta efectuada por el experto a propósito de los delitos que atentan contra la indemnidad sexual.

Artículo L.- Circunstancias agravantes

COMENTARIO:

La pornografía infantil, a pesar de no ser un fenómeno exclusivamente informático, está vinculado al uso de las nuevas tecnologías de la información, pues en la actualidad la mayoría de los comportamientos se perpetran a través de *Internet*, lo cual ha propiciado el aumento en la producción y distribución de la pornografía infantil. Con la inclusión dentro del apartado relativo a la "corrupción de menores" de la pornografía infantil a través de sistemas informáticos se busca evitar, por una parte, la intervención o el uso de menores de edad e incapaces durante el todo el ciclo de tratamiento del material, y por otra, el tráfico o difusión que resulta más fácil, rápido y barato. Entonces, la estructura de este tipo penal se refiere a los actos directos de creación y exhibición, incriminándose la *producción*, es decir la creación, la venta o acto de intermediación, la *distribución* o *divulgación*, y la *exhibición* o acto de ofrecimiento visual directo; y, además, la puesta en circulación de la pornografía infantil que se concreta en la facilitación de las conductas sin importar si son onerosas o gratuitas, públicas o privadas, ni el medio de distribución.

Por otra parte, el artículo L incluye agravantes que se basan en resoluciones y pronunciamientos de organismos internacionales que sirven como asiento para la formulación de políticas de incriminación.

Artículo M. Posesión

COMENTARIO:

El artículo M va vinculado con los dos anteriores como conducta punible que se refiere no a la elaboración y difusión del material pornográfico sino a la simple *posesión*, diferente a la posesión para distribución que se incluiría en el apartado anterior. Por ello se penaliza en un artículo diferente con un castigo atenuado a quien tenga material pornográfico infantil para su uso personal sin haber intervenido en el proceso de producción o distribución, exigiéndose conciencia del sujeto activo de que posee en su sistema u computador los archivos, es decir, un dolo directo.

Artículo N.- Guarda o tutela

COMENTARIO:

Esta norma obedece a motivos Político-criminales. Se recomienda adecuarla a la tipificación general de las conductas que atenten contra la indemnidad sexual.

Artículo O.- Menor o incapaz como destinatario de material pornográfico

COMENTARIO:

Este artículo se dirige a incriminar las conductas en donde los destinatarios directos sean menores de edad o incapaces y no supone la incriminación de conductas genéricas relacionadas con la pornografía. En este sentido, son criterios limitadores que constituyen los elementos típicos esenciales del delito, en primer lugar, los sujetos pasivos, que deben ser menores de dieciocho años y los incapaces; segundo, el tipo queda delimitado a que los actos de difusión, venta o exhibición deben realizarse por medios directos, lo que implica una relación directa e inmediata entre el autor y el sujeto pasivo del delito; por último, además del dolo, debe inferirse un elemento subjetivo del injusto que se concreta en el ánimo lascivo o lúbrico que va vinculado con la relación directa.