ANTEPROYECTO DE LEY DE DELITOS INFORMATICOS

SOMETIDO A CONSULTA PUBLICA POR LA SECRETARIA DE COMUNICACIONES POR RESOLUCIÓN Nº 476/2001 DEL 21.11.2001

Acceso Ilegítimo Informático:

Artículo 1.-

Será reprimido con pena de multa de mil quinientos a treinta mil pesos, si no resultare un delito más severamente penado, el que ilegítimamente y a sabiendas accediere, por cualquier medio, a un sistema o dato informático de carácter privado o público de acceso restringido.

La pena será de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información accedida ilegítimamente.

En el caso de los dos párrafos anteriores, si las conductas se dirigen a sistemas o datos informáticos concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, la pena de prisión será de seis meses a seis años.

Daño Informático

Artículo 2.-

Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier medio, dañare un sistema o dato informático.

Artículo 3.-

En el caso del artículo 2º, la pena será de dos a ocho años de prisión, si mediara cualquiera de las circunstancias siguientes:

1) Ejecutarse el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2) Si fuera cometido contra un sistema o dato informático de valor científico, artístico, cultural o financiero de cualquier administración pública, establecimiento público o de uso público de todo género;

3) Si fuera cometido contra un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Sí del hecho resultaren, además, lesiones de las descritas en los artículos 90 o 91 del Código Penal, la pena será de tres a quince años de prisión, y si resultare la muerte se elevará hasta veinte años de prisión.

Fraude Informático

Artículo 5.-

Será reprimido con prisión de un mes a seis años, el que con ánimo de lucro, para sí o para un tercero, mediante cualquier manipulación o artificio tecnológico semejante de un sistema o dato informático, procure la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

En el caso del párrafo anterior, si el perjuicio recae en alguna administración publica, o entidad financiera, la pena será de dos a ocho años de prisión.

Disposiciones Comunes

Artículo 6.-

1) A los fines de la presente ley se entenderá por sistema informático todo dispositivo o grupo de elementos relacionados que, conforme o no a un programa, realiza el tratamiento automatizado de datos, que implica generar, enviar, recibir, procesar o almacenar información de cualquier forma y por cualquier medio.

2) A los fines de la presente ley se entenderá por dato informático o información, toda representación de hechos, manifestaciones o conceptos en un formato que puede ser tratado por un sistema informático.

3) En todos los casos de los artículos anteriores, si el autor de la conducta se tratare del responsable de la custodia, operación, mantenimiento o seguridad de un sistema o dato informático, la pena se elevará un tercio del máximo y la mitad del mínimo, no pudiendo superar, en ninguno de los casos, los veinticinco años de prisión.

FUNDAMENTOS

La Tecno-era o Era Digital y su producto, la Sociedad de la Información, han provocado un cambio de paradigma social y cultural, impactando drásticamente en la estructura socio-económica y provocando un rediseño de la arquitectura de los negocios y la industria.

La Informática nos rodea y es un fenómeno irreversible. Se encuentra involucrada en todos los ámbitos de la interacción humana, desde los más importantes a los más triviales, generándose lo que, en la doctrina norteamericana, se denomina "computer dependency". Sin la informática las sociedades actuales colapsarían. Es instrumento de expansión ilimitada e inimaginable del hombre y es, a la vez, una nueva de forma de energía, e inclusive, de poder intelectual.

Naturalmente que el Derecho, como orden regulador de conductas, no queda exento del impacto de las nuevas tecnologías, destacándose la imposibilidad de adaptar dócilmente los institutos jurídicos vigentes y los viejos dogmas a estos nuevos fenómenos.

De igual manera, las tecnologías de la información han abierto nuevos horizontes al delincuente, incitando su imaginación, favoreciendo su impunidad y potenciando los efectos del delito convencional. A ello contribuye la facilidad para la comisión y encubrimiento de estas conductas disvaliosas y la dificultad para su descubrimiento, prueba y persecución.

La información, en consecuencia, ha adquirido un valor altísimo desde el punto de vista

económico, constituyéndose en un bien sustrato del tráfico jurídico, con relevancia jurídico-penal por ser posible objeto de conductas delictivas (acceso ilegítimo, sabotaje o daño informático, espionaje informático, etc.) y por ser instrumento de comisión, facilitación, aseguramiento y calificación de los ilícitos tradicionales.

Atendiendo a las características de esta nueva "Era" y sus implicancias ya descriptas, consideramos que el bien jurídico tutelado en los delitos informáticos es la información en todos sus aspectos (vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos), entendiendo que su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todo sus ámbitos y que dependen de los sistemas informáticos (transporte, comercio, sistema financiero, gestión gubernamental, arte, ciencia, relaciones laborales, tecnologías, etc.).

En definitiva, en esta propuesta se entiende por delitos informáticos a aquellas acciones típicas, antijurídicas y culpables que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, en cualquiera de las fases que tienen vinculación con su flujo o tratamiento, contenida en sistemas informáticos de cualquier índole sobre los que operan las maniobras dolosas.

Cabe adelantar que, dentro de estas modalidades de afectación del bien jurídico tutelado, se propone la creación de tres tipos de delitos básicos, con sus correspondientes agravantes, a saber:

a) El acceso ilegítimo informático o intrusismo informático no autorizado (hacking) que supone vulnerar la confidencialidad de la información en sus dos aspectos: exclusividad e intimidad;

b) El daño o sabotaje informático (cracking), conducta ésta que va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información; y

c) El fraude informático, hipótesis en la cual se utiliza el medio informático como instrumento para atentar contra el patrimonio de un tercero, que se incluye en esta ley por su propia especificidad que impone no romper la sistemática de este proyecto de ley especial y por la imposibilidad de incorporarla a los delitos contra la propiedad contemplados en el Código Penal.

Ahora bien, la información, como valor a proteger, ha sido tenida en consideración por el Derecho Penal en otras ocasiones. Sin embargo, se lo ha hecho desde la óptica de la confidencialidad, pero no como un nuevo bien jurídico tutelado abarcativo de varios intereses dignos de protección penal. Piénsese sino en las normativas sobre violación de secretos profesionales o comerciales o la más reciente legislación de Habeas Data, de confidencialidad de la información y en el Derecho Publico Provincial, por las Constituciones de las Provincias del Chaco y de la Rioja, entre otras tantas normas que dentro de regímenes específicos, resguardan a la información con una especial protección.

Asimismo se busca, de alguna manera, cubrir las lagunas legales que fueron quedando luego de la incorporación de cierta protección a determinados intangibles en nuestro derecho positivo nacional.

Se impone aquí aclarar que, como política de legislación criminal, se ha optado por incluir estos delitos en una ley especial y no mediante la introducción de enmiendas al Código Penal, fundamentalmente para no romper el equilibrio de su sistemática y por tratarse de

un bien jurídico novedoso que amerita una especial protección juridico-penal.

Adicionalmente este esquema tiene la bondad de permitir la incorporación de nuevas figuras que hagan a la temática dentro de su mismo seno sin volver a tener que discernir nuevamente con el problema de romper el equilibrio de nuestro Código Penal, que viene siendo objeto de sucesivas modificaciones. Este es el esquema que también han seguido países como los EE.UU. en donde se tiene una alta consciencia de que la carrera tecnológica posibilita nuevas formas de cometer conductas verdaderamente disvaliosas y merecedores de un reproche penal.

Va de suyo, que este no es un anteproyecto general y omnicomprensivo de todas aquellas acciones antijurídicas, sino uno que busca dar una respuesta en un campo especifico del Derecho positivo, como lo es el Derecho Penal.

Desde el primer momento, se decidió privilegiar la claridad expositiva, el equilibrio legislativo y apego al principio de legalidad evitando caer en una legislación errática que terminara meramente en un recogimiento de la casuística local o internacional.

Para ello se debió evitar la tentación de tomar figuras del derecho comparado sin antes desmenuzarlas y analizar estrictamente el contexto en donde se desarrollaron y finalmente ponderar cómo jugarían dentro del esquema criminal general vigente en la República Argentina.

Se buscó, asimismo, llevar nitidez estructural y conceptual a un campo en donde es muy difícil encontrarla, en donde las cuestiones técnicas ofrecen a cada paso claro-oscuros que muchas veces resultan territorios inexplorados no solo para el derecho penal, sino para el derecho en general y sus operadores.

Este anteproyecto abraza el principio de la mínima intervención en materia penal, buscando incriminar únicamente las conductas que representen un disvalor de tal entidad que ameriten movilizar el aparato represivo del Estado. Somos plenamente conscientes de que en más de una oportunidad una ilegitima conducta determinada será merecedora de un castigo extra penal, sea a través del régimen de la responsabilidad civil, del derecho administrativo o la materia contravencional.

Imbuido en este espíritu es que se ha decidido privilegiar el tratamiento de tres tipos delictivos fundamentales. El lector atento podrá notar que no una gran cantidad, sino la mayoría de las conductas que habitualmente se cometen o se buscan cometer dentro del ámbito informático son alcanzadas por alguno de los tipos tratados.

A) ACCESO ILEGITIMO INFORMÁTICO

Se ha optado por incorporar esta figura básica en la que por acceso se entiende todo ingreso no consentido, ilegítimo y a sabiendas, a un sistema o dato informático.

Decimos que es una figura base porque su aplicación se restringe a aquellos supuestos en que no media intención fraudulenta ni voluntad de dañar, limitándose la acción a acceder a un sistema o dato informático que se sabe privado o público de acceso restringido, y del cual no se posee autorización así se concluye que están excluidos de la figura aquellos accesos permitidos por el propietario u otro tenedor legítimo del sistema.

Consideramos apropiada aquí, la fijación de una pena de multa, atento que se trata de una figura básica que generalmente opera como antesala de conductas más graves, por lo que no amerita pena privativa de la libertad, la que por la naturaleza del injusto habría de ser de

muy corta duración.

Este criterio resulta acorde con el de las legislaciones penales más modernas (Alemana, Austríaca, Italiana, Francesa y Española), que ven en la pena de multa el gran sustituto de las penas corporales de corta duración, puesto que no menoscaban bienes personalísimos como la libertad, ni arrancan al individuo de su entorno familiar y social o lo excluyen de su trabajo.

En cuanto a los elementos subjetivos de la figura, se añade un ánimo especial del autor para la configuración del tipo, que es la intencionalidad de acceder a un sistema de carácter restringido, es decir, sin consentimiento expreso o presunto de su titular.

Se contempla en el segundo párrafo, la pena de un mes a dos años de prisión si el autor revelare, divulgare o comercializare la información, como modalidad más gravosa de afectación del bien jurídico tutelado por la circunstancia que supone la efectiva pérdida de la exclusividad de la información, penalidad concordante con la descripción típica introducida por la ley 25.326, la que incorpora al código penal el artículo 157 bis.

Por último, se contempla en el último párrafo, como agravante de ambas modalidades de esta figura delictiva, la circunstancia que los sistemas o datos informáticos sean concernientes a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos, en cuyo caso la pena prevista va desde los seis meses hasta los seis años de prisión. En esta hipótesis resulta palmario el fundamento de la agravante por la importancia que los sistemas e información comprometida involucran para el correcto funcionamiento de servicios vitales para la Nación, sin los cuales se pondría en jaque la convivencia común, en especial en los núcleos urbanos.

B) DAÑO O SABOTAJE INFORMATICO

En cuanto a la protección propiamente dicha de la integridad y disponibilidad de un sistema o dato informático, el artículo propuesto tiene por objeto llenar el vacío que presenta el tipo penal de daño (artículo 183 del Código Penal) que sólo contempla las cosas muebles.

En nuestro país la jurisprudencia sostuvo que el borrado o destrucción de un programa de computación no es una conducta aprehendida por el delito de daño (art. 183 del CP), pues el concepto de cosa es sólo aplicable al soporte y no a su contenido (CNCrimCorrec., Sala 6ta, 30/4/93, "Pinamonti, Orlando M.", JA 1995-III-236). Dicha solución es aplicable también a los datos o información almacenada en un soporte magnético.

Al incluir los sistemas y datos informáticos como objeto de delito de daño se busca penalizar todo ataque, borrado, destrucción o alteración intencional de dichos bienes intangibles. Asimismo, la incriminación tiende también a proteger a los usuarios contra los virus informáticos, caballos de troya, gusanos, cancer routines, bombas lógicas y otras amenazas similares.

La figura proyectada constituye un delito subsidiario, ya que la acción de dañar es uno de los medios generales para la comisión de ilícitos, pero esta subsidiariedad está restringida exclusivamente a los casos en que el delito perpetrado por medio de la acción dañosa esté "más severamente penado".

Asimismo, la ley prevé figuras gravadas, previendo especialmente las consecuencias del daño como, por ejemplo, el producido en un sistema o dato informático concerniente a la seguridad, defensa nacional, salud publica o la prestación de servicios públicos.

En este sentido, conviene precisar el alcance de cada supuesto. Respecto del inciso que agrava el daño a sistemas o datos informáticos con el propósito de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, hemos seguido la técnica legislativa y los supuestos utilizados por el legislador al redactar el artículo 184 inciso 1° del Código Penal.

En segundo término, se protege la información de valor científico, artístico, cultural o financiero de las Universidades, colegios, museos y de toda administración publica, establecimiento público o de uso público de todo género. La especialidad de la información protegida y la condición pública o de uso público de los establecimientos ameritan agravar la pena en estas hipótesis.

En tercer lugar, la conducta se agrava cuando el daño recae sobre un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Aquí, la trascendencia pública, inmanentes a las obligaciones del Estado en materia de seguridad interior y exterior, salud y prestación de servicios públicos, justifican que la sanción penal se eleve por sobre el límite impuesto por la figura básica.

Por último, en función del inciso 3° se contempla como resultado, la producción de una la lesión, grave o gravísima, o la muerte de alguna persona, que pudiere ocurrir con motivo de un daño a un sistema o dato informático, elevándose la pena en función de la elevada jerarquía jurídica que reviste la integridad física de los seres humanos.

Hacemos notar que el Derecho comparado ha seguido los mismos lineamientos, pues frente a la evolución de los sistemas informáticos, las legislaciones penales debieron adaptarse a los nuevos bienes inmateriales.

Así, en la mayoría de los Códigos Penales de los Estados Unidos se ha tipificado una figura de destrucción de datos y sistemas informáticos. También la ley federal de delitos informáticos, denominada Computer Fraud and Abuse Act de 1986, contempla en la Sección (a) (5) la alteración, daño o destrucción de información como un delito autónomo.

El art. 303 a del StGB (Código Penal Alemán) establece que "1. Quien ilícitamente cancelare, ocultare, inutilizare o alterare datos de los previstos en el 202 a, par.2° será castigado con pena privativa de libertad de hasta dos años o con pena de multa".

El art. 126 a del Código Penal de Austria (östStGB) dispone que "1. Quien perjudicare a otro a través de la alteración, cancelación, inutilización u ocultación de datos protegidos automáticamente, confiados o transmitidos, sobre los que carezca en todo o en parte, de disponibilidad, será castigado con pena privativa de libertad de hasta seis meses o con pena de multa de hasta 360 días-multa".

Con la ley N°88-19 del 5 de enero de 1988 Francia incluyó en su Código Penal varios delitos informáticos. Entre ellos, destacamos la figura del art. 462-4 referida a la destrucción de datos que, establecía que "Quien, intencionalmente y con menosprecio de los derechos de los demás, introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o transmisión, será castigado con prisión de tres meses a tres años y con multa de 2.000 a 500.000 francos o con una de los dos penas". Con la reforma penal de 1992, este artículo quedó ubicado en el art. 323-1 del Nouveau Code Pénal, con la siguiente modificación: Se penaliza a quien al acceder a un ordenador de manera fraudulenta, suprima o modifique los datos allí almacenados.

El artículo 392 del Código Penal italiano incluye la alteración, modificación o destrucción

total o parcial de programas de computación y el daño a la operación de un sistema telemático o informático. El artículo 420 del Código Penal, referido a atentados contra sistemas de instalaciones públicas, ha sido también modificado. Actualmente cualquiera que realice un acto con la intención de dañar o destruir sistemas informáticos o telemáticos de instalaciones públicas o sus datos, información o programas puede ser castigado con prisión de uno a cuatro años. En casos de consumación del delito (destrucción o daño a los datos) la pena se eleva de tres a ocho años.

En España, a partir de la reforma del Código penal, el nuevo artículo 264.2 reprime 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.

En 1993 Chile sancionó la ley 19.223 (Diario Oficial de la República de Chile, Lunes 7 de junio de 1993) por la que se tipifican figuras penales relativas a la informática. En su art.3° dispone: "El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio".

C) FRAUDE INFORMATICO

Se ha pensado el delito de fraude informático como un tipo autónomo y no como una figura especial de las previstas en los arts. 172 y 173 del Código Penal. En este sentido, se entendió que en el fraude informático, la conducta disvaliosa del autor está signada por la conjunción de dos elementos típicos ausentes en los tipos tradicionales de fraude previstos en Código: el ánimo de lucro y el perjuicio patrimonial fruto de una transferencia patrimonial no consentida sin que medie engaño ni voluntad humana viciada. El ánimo de lucro es el elemento subjetivo del tipo que distingue el fraude informático de las figuras de acceso ilegítimo informático y daño informático en los casos en que la comisión de las conductas descriptas en estos tipos trae aparejado un perjuicio patrimonial.

El medio comisivo del delito de fraude informático consiste en la manipulación o despliegue de cualquier artificio semejante sobre un sistema o dato informático. Se ha optado por definir la conducta que caracteriza este delito como una "manipulación" o "artificio tecnológico semejante" en el entendimiento de que dichos términos comprenden tanto la acción de supresión, modificación, adulteración o ingreso de información falsa en un sistema o dato informático.

El hecho se agrava cuando el fraude informático recae en alguna Administración Pública Nacional o Provincial, o entidad financiera.

D) Disposiciones Comunes

Como artículo 6°, bajo el título de Disposiciones Comunes, se ha creído necesario, por el tipo de ley especial de que se trata, redactar un glosario que facilite la comprensión de la terminología utilizada por el Anteproyecto.

Se definen en las disposiciones comunes, los dos términos centrales, en torno a los cuales giran los tipos definidos, con el mayor rigorismo a los fines de acotar los tipos en salvaguarda del principio de legalidad, pero, a la vez, con la suficiente flexibilidad y vocabulario técnico, con el objeto de no generar anacronismos en razón de la velocidad con la que se producen los cambios tecnológicos, tratando de aprehender todos los fenómenos de las nuevas tecnologías de la información.

Se ha podido comprobar, fruto de debates que se producen en otras latitudes, que la inmensa cantidad de las conductas ilegitimas que se buscan reprimir atentan ya sea contra uno u otro de estos dos conceptos definidos. Consiguientemente se decidió -siguiendo la Convención del Consejo de Europa sobre Cyber Crime- que, demarcando con nitidez ambos conceptos y haciéndolos jugar dentro de la tipología elegida, se lograba abarcar en mayor medida las conductas reprochables, sin perder claridad ni caer en soluciones vedadas por principios centrales del derecho penal: a saber, Principio de legalidad y Principio de Prohibición de la Analogía.

Independientemente de lo manifestado, se debe tener presente que sí bien el dato informático o información, tal cual está definido en esta ley especial, es sin duda de un intangible, y que -solo o en conjunto con otros intangibles- puede revestir cierto valor económico o de otra índole, no debe, por ello, caerse en el error de -sin mas- asociarlo a lo que en los términos del Derecho de la Propiedad Intelectual se entiende por obra protegida. (vgr. :software). Si bien una obra protegida por el régimen de la Propiedad Intelectual, puede almacenarse o transmitirle a través de red o de un sistema informático y –eventualmente- ser objeto de una conducta de las descripta por esta ley, no toda información – según se define aquí- es una obra de propiedad intelectual y por ende goza del resguardo legal que otorga de dicho régimen de protección especial.

Común a las disposiciones de acceso ilegítimo, daño y fraude informáticos, se ha entendido que el delito se ve agravado cuando quien realiza las conductas delictivas es aquél que tiene a su cargo la custodia u operación del sistema en razón de las responsabilidades y deberes que le incumben, puesto que usa sus conocimientos, status laboral o situación personal para cometer cualesquiera de los delitos tipificados por la presente ley.

En cuanto a la escala penal, se le otorga al juez una amplia discrecionalidad para graduar el aumento de la pena en estos casos, pero le pone un límite, y es que la sanción no podrá superar los veinticinco años de prisión.

Por los motivos expuestos se somete a su consideración el presente anteproyecto de ley.