La criminalidad informática: situación de lege data y lege ferenda en CHILE

RENATO JAVIER JIJENA LEIVA
Profesor de Informática y Derecho. Escuela de Derecho de la Univ. Católica de Valparaíso
(CHILE)

I. La **informática**, que con sus múltiples beneficios revoluciona el devenir histórico de nuestras sociedades, eventualmente puede ser usada con fines delictuales. El hecho de estudiar las implicancias de la informática bajo el prisma del Derecho Penal es, por cierto, una tarea novedosa, que abordamos por considerar que **debido a los radicales cambios que ella ocasiona los nuevos delitos no pueden ser analizados solamente con las categorías tradicionales de la criminología**. Ante las interrogantes de si es necesaria la creación de nuevas formas penales que salgan al paso de posibles extralimitaciones en el uso de la informática, o de si estamos ante un fenómeno tecnológico que requiera la intervención del «ius puniendi» del Estado, la respuesta es, a no dudar, afirmativa. Porque la tecnología computacional, no obstante lo trascendente que ha sido y seguirá siendo para las sociedades modernas, **va camino de convertirse en una variante cada vez más presente en los delitos**, situación que se agrava por cuanto los tipos penales que actualmente existen no subsumen, porque no pueden hacerlo, los hechos ilícitos realizados por medio del computador o en contra de un sistema de tratamiento automatizado de información.

II. Hay quienes estiman que la problemática de los delitos informáticos, sea considerando a la computación sólo como un específico medio de comisión o como el objeto directo de un ilícito informático, ...no constituye un factor criminológico que requiere de la elaboración de tipologías y regula-

ciones específicas. Por cierto que los ilícitos y los abusos informáticos en cierta forma han sorprendido a los penalistas, situación que en parte se debe a que el Derecho Penal anterior al desarrollo de la informática no podía precaver sus implicancias criminales y, además, a que por ser novedoso el tratamiento de esta temática, ella se caracteriza por una notable falta de precisión. En nuestra opinión, tanto para ilustrar a los iuspenalistas como para encontrar la necesaria claridad conceptual, no basta con «aggiornar» esta rama del derecho: Es necesario investigar y desarrollar un Derecho Penal de la Informática.

Consideramos que es insuficiente el pretender que los tipos tradicionales contenidos en la mayoría de los Códigos Penales contemporáneos sean capaces de brindar la protección necesaria. Esto no significa desconocer que algunos de los delitos –sobre todo patrimoniales– pueden ser perpetrados mediante computadores (los que pasan a ser específicas herramientas de comisión). No obstante, por la complejidad del medio informático, por las posibilidades que éste otorga para desarrollar nuevas figuras delictivas o perfeccionar las existentes, por las nuevas modalidades de comisión y porque la legislación penal vigente no puede contemplar todos los posibles delitos informáticos, ...**creemos que es imprescindible tipificar una figura específica, por cierto que sin reformar el Código del ramo** (sostenemos la tesis de que deben consagrarse en leyes específicas que regulen el uso de la informática). La necesidad se basa fundamentalmente en el principio de la tipicidad, una manifestación en materia penal del principio constitucional de legalidad, en cuya virtud no puede haber un delito y no puede asignarse una pena sin que previamente una ley lo haya establecido.

III. El delito informático no ha sido objeto de una elaboración conceptual suficientemente perfilada y, en Chile –en general en los países en que el sistema jurídico es legalista– no basta pretender descansar en la labor creadora de la Jurisprudencia, como ocurre en los países anglosajones. Por la falta de tradición jurídica de la temática en comento, una de las principales trabas para la confección de un tipo legal específico es lo difícil que resulta encontrar una definición «standard», que sea comprensiva de todas las circunstancias que involucra la criminalidad informática. Puede definirse como **toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma** (delito informático propiamente tal).

De la definición surge una primera clasificación. Se llaman delitos **computacionales** a **aquellos** hipótesis en que, tratándose de delitos subsumibles por los tipos tradicionales, la informática es solamente una específica herramienta de comisión que actúa como agravante de la penalidad asignada (V.gr. hurto de valores vía transferencia electrónica de fondos). Son delitos **específicamente informáticos** (V.gr. virus, bombas lógicas o destrucción de infor-

mación, acceso ilícito a los datos, etc.), aquellos en que el objeto material y el bien jurídico afectado es la información tratada automatizadamente. Téngase presente que al tipificarse un delito informático lo que se busca es tutelar el contenido de información (soporte lógico) de un sistema de tratamiento automatizado de la misma y no el soporte físico-tecnológico en que aquel se almacena; así, la apropiación (hurto o robo) o la destrucción (daños o incendio) de un P.C. (Personal Computer), de un disco duro, de un diskette o de una cinta magnética..., independientemente del contenido informacional, son hipótesis perfectamente captables por los tipos del Derecho Penal común.

El concepto de delito informático se ha caracterizado como una acción delictiva en la cual el ordenador es instrumento u objeto del ilícito, definición amplia pero apropiada para acercarse al problema: En algunos casos el computador es objeto del delito; en otros un medio para cometer un hecho delictivo. Se distingue por ende entre los delitos **con medios informáticos**, para aludir a los casos en que la computación es la herramienta o el medio de comisión del hecho punible y los delitos **contra medios informáticos**, cuando pensamos en la lesión del contenido de información de un sistema que será objeto de tratamiento automatizado, o que está siendo procesado o que ya ha sido almacenado y en cómo los datos o programas pueden verse afectados por el delito. Generalmente los delitos contra son cometidos con medios informáticos, pero puede ocurrir que los instrumentos para perpetrarlos no estén vinculados a la tecnología computacional, como cuando acercándole un imán se destruye la información de un disco o de una cinta magnética.

La muy reciente doctrina jurídica que aborda la criminalidad informática distingue básica y sistemáticamente –para analizar los delitos que pueden cometerse en un sistema de tratamiento automatizado de información, sea contra el «hardware» o soporte tecnológico, sea contra el «software» o soporte lógico (programas y datos)– cuatro modalidades: El **«fraude informático»** para aludir a las manipulaciones de programas y datos almacenados, al ingresarlos o al procesarlos; el **«sabotaje informático»** o destrucción o inutilización, sea del equipo o «hardware», sea de los datos o programas (vía programas virus, bombas lógicas, etc.); el **«espionaje informático»** u obtención ilícita de información almacenada –sin autorización– y el **«hurto de horas de computador»**, que consiste en el provecho personal o de terceros que consigue el delincuente al operarlo, sin mediar autorización, fuera del tiempo o del propósito a que está destinado.

IV. Concluímos que el derecho penal debe amparar los contenidos informativos de un sistema, **la información** misma, sin apellidos. Y al no calificarla en un principio **la concebimos genéricamente y proyectable a los restantes bienes jurídicos afectados**: Si la información es nominativa se atenta contra la **intimidad**; de ser económica contra la **propiedad** o el patrimonio; y de ser estratégica o relacionada con la seguridad o la soberanía de un Estado contra lo que hemos denominado la **intimidad nacional**. Pero

además, creemos que la información –el conjunto organizado de datos o el soporte lógico informático– **constituye el objeto material** de un delito informático, no obstante ser intangible e incorporal, con lo cual, retomando la configuración genérica que recién formulamos y para mantener coherencia con la misma, planteamos un doble alcance para la información: **Sería un bien jurídico esencial para la sociedad y se vería afectada directa y materialmente por un ilícito informático**. Por cierto que no sabemos de alguien que comparta este desdoblamiento.

V. Para poner de manifiesto la insuficiencia de los tipos tradicionales, consideremos **el delito de hurto**, que es de apropiación (porque hay un desplazamiento patrimonial) y cometido por medios materiales (con una actividad dirigida a la apropiación de la cosa). Sobre la base del artículo 432 del Código chileno del ramo (la situación es igual en España), el hurto se define como la apropiación de hecho de una cosa mueble ajena, sin la voluntad de su dueño, con ánimo de lucrarse y sin que concurran violencia o intimidación en las personas. Para los efectos de este delito **sólo son cosas** (objeto material) **las corporales que permitan su apoderamiento físico, excluyéndose las inmateriales**, como los derechos, que para el Código Civil también son cosas. Así, este tipo no alcanza a comprender, por ejemplo, la sustracción de datos, por la exigencia de que la apropiación debe recaer sobre una cosa mueble ajena y porque la información es un bien mueble, pero inmaterial, incorporal o intangible, cualquiera que sea el soporte físico informático que la contenga.

Porque no es subsumible en el tipo del Código Penal, el hurto de «software» o del soporte lógico informático requiere de la tipificación de un delito informático. Se trata de contenidos de información, impulsos eléctricos, «bits» (programas y también datos), cuyo valor excede ampliamente al del soporte físico (diskette, cinta) que los contiene.

VI. La única situación actualmente regulada en Chile es el problema de la **«piratería de programas computacionales»**, en virtud de sucesivas modificaciones introducidas a la ley 17.336, sobre propiedad intelectual. Pero esta modalidad de copia ilegal de software **no constituye un delito informático sino que se trata de un delito contra la propiedad intelectual**: El artículo 80, letra b, sanciona a quien intervenga, con ánimo de lucro, en la reproducción, distribución al público o introducción al país y a los que adquieran o tengan con fines de venta programas computacionales.

El Ministerio de Justicia del pasado gobierno, entre 1986 y 1988, elaboró –incurriendo en serios errores de fondo, que ahora no cabe desarrollar– un Proyecto de Legislación Informática, cuerpo prelegislativo en el que se tipificó un delito informático específico. Para el análisis del texto normativo en comento, puede considerarse una cierta evolución, a la cual dedicamos el

Capítulo V de nuestro libro «Chile, la protección penal de la intimidad y el delito informático».

A nuestro parecer, dos son sus **contenidos fundamentales: la regulación del tratamiento automatizado de información nominativa y la criminalidad informática.** El artículo 1.º se extiende en la descripción de los datos amparados por el proyecto (ámbito de aplicación), aludiendo específicamente a los datos personales, los de familia y los concernientes a los derechos y deberes garantizados por la Constitución Política. Un informe técnico señaló que el proyecto en estudio se refería a la recolección y difusión informática de datos personales, es decir, datos que permiten la identificación del sujeto al que se refieren, quedando los demás al margen de esta legislación. Despejando toda duda interpretativa, consignaba que era la aplicación de la informática la que hacía necesaria la promulgación de una ley que cautelara y protegiera la vida privada de las personas. Sin lugar a dudas que **el mayor logro lo constituyó el haber insertado en una ley de protección de datos un específico tipo de delito informático**, en que el objeto material afectado es el soporte lógico del sistema, ...la información (datos y, necesariamente, los programas) destinada a ser procesada, durante su procesamiento o contenida en un sistema computacional.

El **artículo 30** supone la comisión con medios informáticos de los delitos contemplados en la legislación penal, agravándose su penalidad (agravante especial). Esta figura, que tácita o indirectamente vino a modificar el CP., estimamos que se presenta como un complemento importante al delito tipificado en el artículo 31, por cuanto evita posibles dudas o vacíos de interpretación y amplía la protección penal de los bienes jurídicos que eventualmente pueden verse afectados por la criminalidad informática.

El **artículo 31** es el más importante, por cuanto tipifica en forma amplia un delito específico o propiamente informático, señalando: «Comete delito informático el que maliciosamente y sin derecho o autorización realice cualquier acto con la finalidad de obtener acceso, de apoderarse, de destruir o inutilizar, transformar o desfigurar la información contenida o destinada a ser procesada, en todo o en parte, en un sistema automatizado de tratamiento de la misma; o con la finalidad de impedir u obstaculizar el normal procesamiento de los datos contenidos en un sistema automatizado; o con la finalidad de revelar o transmitir indebidamente información. El culpable de este delito será sancionado con la pena de presidio menor en su grado medio a presidio mayor en su grado mínimo, según la extensión o cuantía del daño causado».

– Se considera en el tipo que tres pueden ser los fines posibles del autor del delito. Analizándolos, claramente se observa cómo se ampararon los datos en los diferentes estados en que pueden encontrarse: a) La información destinada a ser procesada; b) Durante su «normal procesamiento», y c) La información contenida en un sistema informático.

El **artículo 32** introduce otro tipo penal, el que consideramos bastante

cuestionable. La norma señala: «Igualmente comete delito informático el que organice o utilice un sistema de tratamiento automatizado de información con un propósito ilícito. El culpable de este delito sufrirá las penas del artículo 293 del CP».

– Este artículo derechamente es atacable de inconstitucionalidad por falta de tipicidad, en consideración a lo que dispone el artículo 19 N°3, inciso 8° de la Constitución Política de 1980. En efecto, allí se establece que la Constitución asegura a todas las personas, N°3: «La igual protección de la ley en el ejercicio de sus derechos». En materia penal esta igualdad está desarrollada en los incisos 7° y 8°, señalando el segundo que «ninguna ley podrá establecer penas sin que la conducta que se sanciona esté expresamente descrita en ella». Precisamente, el artículo 32 del proyecto no describe expresamente la conducta en él sancionada, cuando utiliza como parte de la hipótesis de hecho, la expresión **«con un propósito ilícito»**.

VII. El cuerpo prelegislativo en comento ha sido recogido por los actuales parlamentarios chilenos, en una moción de ley que debiera ser colocada en tabla durante el presente año, para su análisis en la Comisión de Constitución, Legislación y Justicia de la Cámara de Diputados. Por lo mismo, para terminar y en un plano de «lege ferenda» o de «ideas sobre cómo legislar», queremos formular los siguientes alcances que deberán considerarse:

– Frente a conductas en que dolosamente se atente contra el contenido de información de un sistema informático –no sólo nominativo–, la tutela requerida pasa por la tipificación de hipótesis de **delitos informáticos**, también insertos en una ley de protección de datos.

– Valorativamente, la intimidad, la información nominativa, es el más relevante de los bienes jurídicos afectados por la criminalidad informática. En Chile, algunos abogados que incluso participaron en la revisión del proyecto en comento, descartan la tutela penal de la intimidad –vía delitos informáticos– y consideran de mayor relevancia al patrimonio, ...porque los perjuicios económicos suelen ser considerables. No obstante ser importante la criminalidad patrimonial informática, se trata de una opción que no podemos, por formación y convicción, compartir. Cuando se viola computacionalmente una garantía de rango constitucional, un derecho primordial para la dignidad, libertad y seguridad de las personas, deben poder aplicarse las sanciones más drásticas que contempla un ordenamiento jurídico, es decir, las penales, que implican privación de libertad; y éstas deben tipificarse.

– **Tampoco existe discusión doctrinaria alguna sobre si los atentados contra la intimidad deben ser ilícitos civiles o penales**. Hay quienes señalan que las conductas «negligentes o culposas» debieran ser sancionadas en sede de responsabilidad civil, descartándose la tipificación de cuasidelitos informáticos. Pero no sabemos de nadie, después de seis años de investiga-

ción en Chile y en el extranjero, que afirme que las conductas «dolosas» no deban sancionarse penalmente: para efectos del resarcimiento por la intromisión dolosa en la intimidad de una persona, se requiere que el hecho sea constitutivo de delito; así, «la configuración del delito informático como una figura punible distinta, es la única solución que permitirá resolver el problema desde el punto de vista del hecho ilícito».