Autor: Dra. Esc. María José Viega Rodríguez

Doctora en Derecho y Ciencias Sociales
Escribana Pública
Aspirante a la Cátedra de Informática Jurídica Fac. de D. y Ciencias Sociales (UR)
Integrante del Instituto de Derecho Informático de la Fac. de D. Y Ciencias Sociales (UR)
Integrante de la Comisión de Derecho Informático y Tecnológico de la Asociación de Escribanos del Uruguay

E-mail: mjviega@adinet.com.uy

Título del trabajo: "Un nuevo desafío jurídico: Los Delitos Informáticos"

Abstract:

Conceptos. Conveniencia de legislar. Clasificación. Caracterización de los sujetos. Enumeración ilustrativa de los más conocidos. Derecho comparado. Legislación Internacional y nacional.

Area temática: Comisión de Delitos informáticos.

UN NUEVO DESAFIO JURIDICO: LOS DELITOS INFORMATICOS

Dra. Esc. María José Viega Rodríguez

mjviega@adinet.com.uy

Abstract: *Conceptos. Conveniencia de legislar. Clasificación. Caracterización de los sujetos. Enumeración ilustrativa de los más conocidos. Derecho comparado. Legislación Internacional y nacional.*

Trabajo inédito

I. Concepto de delito informático.

Esta ponencia tiene como objeto compartir con ustedes mi inquietud en relación a uno de los tantos desafíos que la informática ha planteado al derecho. Y si bien en nuestro país ya hace unos cuantos años que existen proyectos a nivel legislativo aún no se ha legislado sobre este tema.

Estamos frente a un aspecto negativo del desarrollo tecnológico que son los delitos informáticos. Ellos son la consecuencia de las nuevas posibilidades que la informática plantea, en este caso en el ámbito de conductas delictivas. Las computadoras nos ofrecen otras formas de infringir la ley, y por lo tanto hoy se pueden cometer delitos tradicionales de una manera muy sofisticada. Por esta razón es importante dilucidar si existen o deben existir delitos informáticos específicos, lo que implica tener en cuenta si las figuras tipificadas en nuestro Código Penal se adecuan a estos, o si por el contrario necesitaremos tipificar nuevos delitos.

En la Universidad de México se ha realizado un estudio sobre este tema y se define a los delitos informáticos como: "*todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático*".

Jijena Leiva los define 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*".[1]

La Organización para la Cooperación Económica y el Desarrollo (OECD) da una definición que es considerada como "abarcante" y lo define como: "*cualquier conducta, no ética, o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos*".[2]

Se ha dicho que los llamados delitos informáticos no constituyen una nueva categoría delictiva, sino que son los mismos delitos que ya se vienen castigando: delitos contra las personas, contra el honor, la libertad, la seguridad pública o la Nación.

Se ha tratado de encuadrar los delitos informáticos dentro de los delitos como son: robo, hurto, fraudes, falsificaciones, estafa, sabotaje, etc, pero debemos analizar si las categorías tradicionales son adecuadas o no respecto a estas modalidades delictivas.

En mi opinión los delitos informáticos se pueden definir como toda conducta ilícita, sancionada por el derecho penal, para la realización de la cual se utilizan los medios informáticos, frutos de las nuevas tecnologías, ya sea como herramienta para la comisión del delito o como fin en sí mismo, afectando los datos contenidos en un sistema.

II. Existencia de los delitos informáticos, ¿es conveniente legislar?

El derecho penal puede asumir diferentes posiciones en relación a las consecuencias de la informática, entre las cuales podemos destacar:

a) No sería necesario crear en nuestro país delitos informáticos específicos, porque los delitos convencionales ampararía las diferentes posibilidades delictivas.
b) Los delitos convencionales que estén relacionados con un sistema de computación, los convertiría por ello en un delito informático. Razón por la cual no sería necesario crear nuevos delitos, sino que habría que valorar el grado en que se utilizó la tecnología como medio u objeto del delito.
c) Los delitos convencionales son insuficientes para enfrentar la delincuencia informática. Dice Nahum Bergtein[3] que los sistemas de computación han provocado una metamorfosis en el seno de la sociedad, que conduce a mejorar la calidad de vida, pero es susceptible de provocar daño o peligro de daño a bienes jurídicos que pueden o no estar personalmente tutelados.

Personalmente creo en la existencia de los delitos informáticos como tales, con una estructura propia y carentes, en el derecho uruguayo de normativa jurídica. La información no es un bien que se encuentre protegido en nuestro derecho, salvo excepciones muy concretas como el caso del secreto profesional y el secreto de Estado. Otro elemento a tener en cuenta es que esta clase de delitos se concretan en la mayoría de los casos como delitos a distancia, una forma jurídica que hasta hoy era casi inaplicable. Y la distancia va a estar dada desde dos puntos de vistas: geográfico y temporal. Y es fundamental el principio "*hullum crime sine praevia lege*", "*Nulla pena sine lege*", establecido en nuestro artículo primero del Código Penal en el que se establece: "es delito toda acción u omisión expresamente prevista por la ley Penal. Para que ésta se considere tal, debe contener una norma y una sanción". Obviar esto nos lleva a infringir el principio de legalidad y ha realizar interpretaciones extensivas de la norma.

III. Clasificación.

Los delitos informáticos han sido objeto de variadísimas clasificaciones, y se han tenido en cuenta a estos efectos:

- el perjuicio causado
- el papel que el computador desempeñe en la realización del mismo
- el modo de actuar
- el tipo penal en que se encuadren
- clase de actividad que implique según los datos involucrados.

Julio Tellez Valdes clasifica a los delitos informáticos en base a dos criterios:

1. como instrumento o medio: se tienen a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.
2. como fin u objetivo: se enmarcan a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

María de la Luz Lima: clasifica los delitos electrónicos en tres categorías, de acuerdo a como utilizan la tecnología electrónica:

1. Como método: cuando los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. Como medio: en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

Jorge Pacheco Klein distingue:

1. Delitos informáticos internos. Ej.: sabotaje de programas.
2. Delitos a través de las telecomunicaciones. Ej.: hacking.
3. Manipulación de computadoras. Ej.: apropiación indebida, peculado y fraudes informáticos. Es la más vinculada a delitos de cuello blanco.
4. Utilización de computadoras en apoyo a empresas criminales, como el lavado de dinero y la distribución ilícita de drogas.
5. Robos de software(piratería).

IV. Caracterización de los Sujetos

Sujeto Activo.

No estamos hablando de delincuentes comunes. Los sujetos activos tienen como características:

a) Poseen importantes conocimientos de informática.

b) Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible (se los ha denominado *delitos ocupacionales* ya que se cometen por la ocupación que se tiene y el acceso al sistema.

c) A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar el sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

d) Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

e) Estos delitos se han calificado de "cuello blanco", porque el sujeto que comete el delito es una persona de cierto status socioeconómico.

La "**cifra negra**" es muy alta. No es fácil descubrirlo ni sancionarlo, en razón del poder económico de quienes lo cometen y también es importante destacar que los daños económicos son altísimos. Se habla de pérdidas anuales por delitos informáticos y otros tecno-crímenes, que van desde los U$S 100 millones (Cámara de Comercio de los Estados Unidos) hasta la suma de U$S 5.000 millones, de acuerdo a un estudio de 1990 hecho por una firma auditora.

Pacheco Klein nos dice: *"Otro estudio estimó que sólo el 1% de los robos de computadora son detectados, y quizá sólo un 15 % de ellos sean denunciados. Cuando los delitos informáticos son denunciados y llevados a juicio, muchos de ellos son negociados fuera del juzgado; sólo alrededor del 24 % van realmente a juicio, y alrededor de dos tercios de esos juicios resultan en la absolución y el archivo del expediente."*

Un punto muy importante es que la opinión pública no considera delincuentes a estos sujetos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario el autor de estos delitos distingue entre el daño a las personas (que es inmoral) y el daño a las organizaciones, porque en este último caso sienten que "hacen justicia", se le ha llamado a este punto de vista el *síndrome de Robin Hood*.

Esto no nos es ajeno a los uruguayos, y creo que este llamado "síndrome" en realidad es una opinión social generalizada. Y si algo tengo muy claro es que no se evitarán los delitos informáticos con una ley que establezca severas penas, sino que los temas deben ser debatidos socialmente, debemos educar a las personas acerca del alcance de las actividades informáticas, debemos crear conciencia a través de la educación y no del miedo. En este tema podemos hacer un paralelo con las

fotocopias, que si bien existe una Ley de derechos de autor y una Ley del Libro, primó el interés social, primó el derecho a educarse, porque no creo que en este tema exista una falta de conciencia de que la fotocopia perjudica al autor, sino que en cierta forma el autor está devolviendo a esa sociedad lo que la misma le ha dado.

Sujeto Pasivo.

Es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo.
Como ya dijimos anteriormente, la mayor parte de los delitos informáticos no son descubiertos o denunciados a las autoridades responsables, las empresas o bancos tienen miedo al desprestigio y su consecuente pérdida económica.

V. Tipos de delitos informáticos conocidos.

Esta no pretende ser una clasificación con un criterio metodológico propio, sino simplemente una enumeración ilustrativa que he realizado de los delitos informáticos que se conocen, para dar un pantallazo general de las distintas formas en que los mismos pueden cometerse.

1) Robos, hurtos, vaciamientos, desfalcos, estafas o fraudes cometidos mediante manipulación y uso de computadoras.

a) Manipulación de los datos de entrada – insiders.

Estamos ante un fraude informático, conocido también como sustracción de datos y estamos ante el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

b) La manipulación de programas.

Otro caso muy difícil de descubrir y a menudo pasa inadvertido debido a que el sujeto activo en este caso debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora en forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal. El nombre se debe al episodio de la Ilíada de Homero, Ulises urdió una estratagema en virtud de la cual le regala a los troyanos un gran caballo de madera, que en el interior ocultaba soldados, haciendo creer que el ejército griego abandonaba el sitio de la ciudad. El caballo entró en el recinto amurallado de Troya y aprovechando la noche y la confianza de los habitantes, los guerreros ocultos hicieron entrar a las tropas griegas que aguardaban en las puertas de la ciudad.

c) Manipulación de los datos de salida – outsiders.

El caso de manipulación más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a partir de tarjetas bancarias robadas, sin embargo, hoy en día se usan equipos y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d) Fraude efectuado por manipulación informática. Técnica del Salami.

Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salami" en la que cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se transfieren a otra. Esta modalidad de fraude informático se realiza sin grandes dificultades y es muy difícil de detectar. Uno de los casos más ingeniosos en el “redondeo hacia abajo”, que consiste en una instrucción que se le da al sistema informático para que transfiera a una determinada cuenta los centavos que se descuenten por el redondeo.

2) Fraudes contra sistemas, daños o modificaciones de programas o datos computarizados.

a) Sabotaje informático.

Consiste en borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

Virus.

Un virus es un programa que puede ingresar en un sistema a través de cualquiera de los métodos de acceso de información externa, se instala, se reproduce y causa daño. La gravedad de los virus es variable, puede ser simplemente una molestia en la pantalla, como el caso del “ping-pong” y también existen aquellos que pueden llegar a eliminar el contenido de una base de datos.

Entre los virus más conocidos tenemos, a modo de ejemplo:

⇒ ping-pong: consiste en un punto que se mueve por toda la pantalla y parece rebotar en los bordes.

⇒ Datacrime o virus del viernes 13 el virus Jerusalem estaba destinado para destruir todas las memorias militares y científicas de Israel el 13 de mayo de 1988.

⇒ Michelangelo: este último de fama más reciente.

Actualmente existe una gran carrera entre aquellos que crean los virus y los que desarrollan los antivirus. Hasta ha llegado a decirse que los virus son desarrollados por los mismos productores de antivirus, ya que hoy en día es fundamental adquirir antivirus y los mismos deben ser renovados constantemente, por supuesto que no existe ninguna prueba concreta.

Gusanos.

Se fabrica de forma análoga al virus, se infiltra en los programas ya sea para modificar o destruir los datos, pero se diferencia de los virus porque no pueden regenerarse. Las consecuencias del ataque de un gusano pueden ser graves, por ejemplo un programa gusano puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita y luego se destruirá.

Rutinas cáncer.

Guibourg[5] las define como aquellas que *“distorcionan el funcionamiento del programa y se autorreproducen al estilo de las células orgánicas alcanzadas por un tumor maligno”*

Bomba lógica o cronológica.

Consiste en la introducción en un programa de un conjunto de instrucciones indebidas que van a actuar en determinada fecha o circunstancia, destruyendo datos del ordenador, distorsionando el funcionamiento del sistema o paralizando el mismo. Las bombas lógicas son difíciles de detectar antes de que exploten, son las que pueden resultar más dañinas y preveer que exploten cuando el

delincuente ya se encuentre lejos. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla la bomba.

b) Acceso no autorizado a Sistemas o Servicios.

Puede darse por motivos diferentes: desde la simple curiosidad, como en el caso de muchos piratas informáticos (Hacker) hasta el sabotaje o espionaje informático. Estos ingresos no autorizados comprometen la integridad y la confidencialidad de los datos. Podríamos llegar hasta actos de atentados terroristas, por ejemplo en el caso de intervenir sistemas de tráfico aéreo.

c) Espionaje – Acceso telemático no autorizado a un sistema - Hackers – Fuga de datos.

El espionaje es la obtención de información a través de medios informáticos para ser utilizada posteriormente normalmente para la obtención de beneficios económicos de enorme magnitud.

El acceso puede darse en forma directa, por ejemplo cuando un empleado accede en forma no autorizada, estamos frente a un riesgo interno. Pero se puede acceder en forma indirecta, o sea a través de una terminal remota.

El delincuente puede aprovechar la falta de medidas de seguridad para obtener acceso o puede descubrirle las deficiencias a las medidas existentes de seguridad. A menudo, los hackers se hacen pasar por usuarios legítimos del sistema, esto suele suceder debido a la frecuencia en que los usuarios utilizan contraseñas comunes.

La fuga de datos consiste en la versión informática de las tradicionales prácticas de “espionaje industrial”

El acceso no autorizado a sistemas informáticos reviste diversas modalidades, que son:

Puertas falsas: Se trata de intromisión indebida a los sistemas informáticos aprovechando los accesos o “puertas” de entrada, que no están previstas en las instrucciones de la aplicación, pero que facilitan la revisión o permiten recuperar información en casos de errores de sistemas. También llamadas “puertas trampa” porque permiten a los programadores producir rupturas en el código y posibilitar accesos futuros.

Llave maestra (Superzapping). Consiste en el uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático. El nombre proviene de un programa de utilidad que se llama superzap, que permite abrir cualquier archivo de una computadora aunque se halle protegido por medidas de seguridad.

Pinchado de líneas. Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas.

Clasificación del pirata informático[6]:

Hacker: persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del operador común, que en general, se conforma con aprender lo básico.

Cracker: aquel que rompe con la seguridad de un sistema. El término fue acuñado por Hacker en 1985, oponiéndose al mal uso de la palabra Hacker por parte de la prensa.

Preaker: arte y ciencia de crackear la red telefónica para obtener beneficios personales (por ejemplo llamadas gratis de larga distancia).

d) Reproducción no autorizada de programas informáticos - Piratería.

"*Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual*"[7]

3) Falsificaciones Informáticas.

- **Como objeto.**

Cuando se alteran datos de los documentos almacenados en forma computarizada. Pueden falsificarse o adulterarse también microformas, microduplicados y microcopias; esto puede llevarse a cabo en el proceso de copiado o en cualquier otro momento.

- **Como instrumentos.**

Las computadoras pueden utilizarse para realizar falsificaciones de documentos de uso comercial. Las fotocopiadoras computarizadas en color a base de rayos láser dio lugar a nuevas falsificaciones. Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos, crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.

4) Datos personales. Delito de violación a la intimidad.

Consiste en la violación de la intimidad de la vida personal y familiar ya sea observando, escuchando o registrando hechos, palabras, escritos o imágenes, valiéndose de instrumentos, procesos técnicos u otros medios.

También se podría tipificar como delito el que organiza, proporciona o emplea indebidamente un archivo que tenga datos referentes a las convicciones religiosas, políticas o a la vida íntima de las personas.

5) Homicilio.

Aunque no parezca creíble es posible cometer homicidio por computadora. Se daría en los casos en que a un paciente que está recibiendo un determinado tratamiento, se modifican las instrucciones en la computadora, que puede hacerse incluso desde una terminar remota.

6) Interceptación de comunicaciones (browsing).

Mediante la conexión en paralelo de terminales no autorizadas se puede acceder a datos e incluso manipular la información.

7) Robo de servicios

a) **Robo de servicios o Hurto de tiempo** de ordenador. Cuando los empleados utilizan en una empresa horas de máquina sin autorización para realizar trabajos personales. Hoy en día este tipo de delito ha caído en desuso, ya que con la existencia de las PC y lo que ha bajado su costo, resulta sencillo tener acceso a una computadora, pero esto no era así hace unos años cuando las grandes computadoras eran propiedad de las empresas debido al alto costo de las mismas.

b) **Apropiación de informaciones residuales** que han sido abandonadas por sus legítimos usuarios de servicios informáticos como residuo de determinadas operaciones.

c) **Parasitismo informático.** Se alude a las conductas que tienen por objeto el acceso ilícito a los equipos físicos o a los programas informáticos, para utilizarlos en beneficio del

delincuente. Suele asociarse a esta figura la de la *Suplantación de personal* que se refiere a toda la tipología de conductas en las que los delincuentes sustituyen a los legítimos usuarios informáticos. Un ejemplo es el referente al uso ilícito de tarjetas de crédito.

8) Hurto calificado por transacciones electrónicas de fondos

Este es el caso del hurto que se comete mediante la utilización de sistemas de transferencia electrónica de fondos, de la telemática en general, o también cuando se viola el empleo de claves secretas. Este es un delito tipificado en Perú, que en la doctrina y legislación comparada está tipificado como fraude informático.

9) Delitos de daño aplicable al hardware

El robo de un establecimiento comercial de una o varias computadoras no constituye un delito informático, pero sí el daño o sabotaje al hardware que impide la puesta en marcha de un sistema informatizado de diagnóstico médico. Este tipo de delitos está pensado para bienes materiales y no inmateriales. Puede darse un atentado contra la máquina o sus accesorios (discos, cintas, terminales, etc.)

VI. Derecho comparado.

Me interesa destacar como algunos países han encarado este tema, para que nos sirva de referencia a los efectos de llegar a posibles soluciones que puedan resultar viables:

Alemania

A partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica en la que se contemplan los siguientes delitos:

- Espionaje de datos
- Estafa informática

Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos.

Alteración de datos, es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

Sabotaje informático, destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

Utilización abusiva de cheques o tarjetas de crédito

Austria

Ley de reforma del Código Penal de 22 de diciembre de 1987.
Contempla los siguientes delitos:

Destrucción de datos, no solo datos personales sino también los no personales y los programas.

Estafa informática, se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Francia

La Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

Acceso fraudulento a un sistema de elaboración de datos: Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

Sabotaje Informático: Falsear el funcionamiento de un sistema de tratamiento automático de datos.

Destrucción de datos: Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Falsificación de documentos informatizados: Se sanciona a quien de cualquier modo falsifique los documentos informatizados con intención de causar un perjuicio a otro.

Estados Unidos

Estados Unidos en 1994 modificó con el Acta Federal de Abuso Computacional su antecedente, el Acta de Fraude y Abuso Computacional de 1986.

Modifica el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos; para ambos impone además de la aplicación de multa, un año de prisión para los primeros y 10 años para los segundos.

Se contempla la regulación de los virus, conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir. Copiar transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas.

Inglaterra

Computer Misuse Act del año 1990: introdujo el delito de acceso no autorizado. Dice Pacheco Klein que: “Esta cláusula de la ley fue, principalmente, una reacción a la publicidad y al medio en torno a los virus de las computadoras. El artículo 3º inciso 2º establece que la persona tiene que tener intención de “modificar el contenido de cualquier computadora”, y de esa manera:

a) Impedir la operación de cualquier computadora; o
b) Impedir o dificultar el acceso a cualquier programa, o la confianza de esos datos.
c) Impedir la ejecución de cualquiera de esos programas, o la confianza en esos datos.”

La ley fue criticada por su amplitud, sin embargo la obtención de evidencia desde lugares remotos ha creado problemas en la legislación inglesa.

En 1994 la ley fue reformada para permitir el acceso a la policía y a las agencias especializadas del orden a los boletines informativos.

España

Nuevo Código Penal español

Artículo 255: sanciona cualquier actividad artificiosa o que induzca en error a una máquina. Esta conducta puede darse en los siguientes casos:

1. Tomar ventaja de mecanismos ya instalados, por ejemplo, abusar de sistemas informáticos o violar las reglas preestablecidas para el uso del teléfono;
2. Alterar en forma ilegal cualquier aparato de medición, interrumpiendo de esa manera dañosa el funcionamiento del mecanismo. En nuestro derecho existe una norma similar que regula los casos de hurto de energía eléctrica, a través de la manipulación de contadores.

3. Usar cualquier otra forma secreta para alterar una máquina o mecanismo.

Artículo 256: castiga a quienes cometan fraude a través de los sistemas de computación.

Perú

El ordenamiento jurídico peruano tipifica los siguientes delitos, los cuales se encuentran dentro del concepto de delitos informáticos que hemos dado en la primera parte de este trabajo.
Ellos son:

Delito de violación a la intimidad (art. 154 del Código Penal),
Delito de hurto calificado por transferencia electrónica de fondos (art. 186 segundo párrafo numeral 3 del Código Penal, modificado por Ley 16.319),
Delitos contra los derechos de autor (art. 216 Código Penal),
Delito de falsificación de documentos informáticos (Decreto Legislativo 681, art. 19 – art. 427 del Código Penal),
Delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos (art. 198 inc. 8 del Código Penal),
Delito de daños aplicable al hardware (art. 205 del Código Penal)

VII. Legislación Internacional.

Un elemento importante a tener en cuenta es que muchas veces el delito se va a convertir en un "caso internacional", ya que las redes transmisoras de datos permiten con gran facilidad el flujo de la información fuera de las fronteras del Estado.

GATT.- Acuerdo de la Ronda Uruguay de Aranceles Aduaneros y Comercio, art. 10 relativo a los programas de ordenador y compilaciones de datos, serán protegidos como obras literarias de conformidad con el Convenio de Berna para la protección de obras Literarias y Artísticas.

Convención para la Protección y Producción de Phonogramas.

Convención relativa a la Distribución de Programas y Señales.

Convenios de la OMPI.

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el uso indebido de los programas de computación.

Hay que tener en cuenta que las posibles implicaciones de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de legislación unificada que, facilita la comisión de los delitos.

En 1986 la OCDE publicó un informe *titulado Delitos de informática: análisis de la normativa jurídica*, donde se señalan las normativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos.

VIII. Legislación Nacional.

a) Aplicación de delitos del código Penal

Hurto.

Artículo 340. *"El que se apoderare de cosa ajena mueble, sustrayéndosela a su tenedor, para aprovecharse o hacer que otro se aproveche de ella, será castigado con tres meses de prisión a seis años de penitenciaría."*

El problema está planteado con el objeto, o sea la cosa ajena mueble. En nuestro derecho fue necesario agregar por el artículo 316 de la ley 13.737 el Hurto de Energía y Agua Potable (art. 343 del Código Penal).

Teniendo presente el principio de legalidad, este artículo no es aplicable a los casos de hurto de información, por ejemplo, donde la misma no se sustrae a su tenedor, sino que este sigue teniéndola. Tampoco se aplica al dinero contable que contiene una transferencia electrónica de fondos, porque no estamos en presencia de una cosa mueble.

Estafa.

Artículo 347. *"El que con estratagemas o engaños artificiosos, indujere en error a alguna persona, para procurarse a sí mismo o a un tercero, un provecho injusto, será castigado con seis meses de prisión a cuatro años de penitenciaría"*.

Se ha discutido acerca de si se puede engañar a una máquina, o si por el contrario la víctima de la estafa debe ser una persona. Se ha dicho que no puede engañarse a una máquina, sin embargo hoy existe una nueva interpretación que establece que detrás de la máquina hay una persona que la diseñó y es el programador.

Daño.

Artículo 358. *"El que destruyere, deteriorare o de cualquier manera inutilizare, en todo o en parte, alguna cosa mueble o inmueble ajena, será castigado, a denuncia de parte, cuando el hecho no constituya delito más grave con multa de ....."*

El objeto del daño debe ser una cosa mueble o inmueble, los delitos informáticos dañan a los datos, a la información, a los programas, pero no a la computadora en sí. En virtud de esto sería imposible aplicar este artículo al daño informático. Además se habla de dañar cosa ajena, y aquí en realidad el propietario del soporte físico (la computadora) es en la mayoría de los casos el usuario.

b) Proyecto de ley presentado por el senador Prof. Alberto Traversoni.

Este primer proyecto data de noviembre del año 1987 y contaba de 3 artículos que se transcriben a continuación:

"*Art. 1. El que en forma maliciosa, a conciencia y sin autorización intercepta, interfiere, recibe, usa, altera o destruye un computador, un sistema o red de computadores, un soporte lógico o programa o una base de datos en todo o en parte, con la finalidad de defraudar, causar perjuicios a terceros, obtener lucro, bienes o información, comete delito informático.*

Art. 2. El autor de tales delitos será castigado con 2 años a 6 años de penitenciaría. Es un agravante la circunstancia de que dicho delito sea cometido por un funcionario público en el ejercicio de sus funciones.

Art. 3. Los coautores y cómplices, con relación a la pena, se les aplicará los artículos 88 y 89 del Código Penal."

c) **Proyecto de ley presentado por Pacheco Klein.**

El proyecto que se transcribe y comenta fue presentado en la legislatura pasada y el mismo no fue aprobado.

Art. 1º. (Acceso doloso). El que en forma intencional, sin la debida autorización o excediendo la misma, interceptare, interfiriere, recibiere, usare, alterare, dañare o destruyere, un sistema o red de computadoras, un soporte lógico, programa de software o base de datos, en todo o en parte, será castigado con dos a cuatro años de penitenciaria.

Si el hecho tuviere por objeto el procurarse un beneficio indebido de acuerdo a la ley, para sí o para un tercero, se castigará con dos a seis años de penitenciaría.

Para la aplicación de la pena, el juez deberá tener en cuenta el monto o la cuantía del perjuicio ocasionado.

El bien jurídico tutelado por esta norma es la propiedad y la privacidad de las personas, agredida en forma dolosa, a través de la ejecución de los verbos nucleares interceptar, recibir, usar, alterar o destruir. Sería importante establecer agravantes, además de la calidad de funcionario público que veremos más adelante, cuando se trata de datos personales, como se ha previsto en la legislación peruana, en casos en que se utiliza algún medio de comunicación social. También en España se castiga más severamente a quien difunde o revela a terceros los datos obtenidos. Se consideran además, causas agravantes cuando la violación de la intimidad tenga por objeto datos personales "sensibles", o sea: ideológicos, religiosos, sexuales, raciales, sanitarios, o cuando la víctima es menor de edad o incapaz.

Art. 2º. (Acceso culposo) El que en forma culposa, por no prever un resultado previsible, sin la debida autorización o excediendo la misma, accediere, interceptare, interfiriere, recibiere, usare, alterare, dañare o destruyere un sistema o red de computadoras, un soporte lógico, programa de software o base de datos, en todo o en parte, será castigado con veinticinco meses de prisión a tres años de penitenciaría.

Para la aplicación de la pena, el juez deberá tener en cuenta el monto o la cuantía del perjuicio ocasionado.

En este artículo, a diferencia con el 1º se incrimina a título de culpa, por no prever un resultado previsible, debido a la negligencia, imprudencia, impericia o por desobedecer las leyes o reglamento. El bien jurídico protegido es igual a la anterior y tiene un verbo nuclear más que es "acceder".

Artículo 3º. Fraude informático El que con intención de procurarse a sí mismo o a un tercero un beneficio patrimonial indebido, causare un perjuicio en el patrimonio de otro, operando un proceso de datos incorrecto, configurando incorrectamente un programa de software, empleando adrede datos falsos, incorrectos o incompletos, o a través de cualquier otra intervención o manipulación ilegítima, sin la debida autorización o excediendo la misma, será castigado con pena de dos a seis años de penitenciaría.

Esta norma la toma Pacheco Klein del derecho alemán para prever la estafa en el ámbito informático. El bien jurídico protegido es la propiedad y se incrimina a título de dolo.

Artículo 4º. Hurto informático El que utilizando un sistema de computación, soporte lógico o software adecuado, sin la debida autorización, o excediendo el marco de la misma, se apoderare de valores intangibles o incorporales ajenos, como ser depósitos monetarios, transferencias electrónicas de fondos, créditos, información y/o secretos industriales o comerciales, sustrayéndoselos a su tenedor, para aprovecharse o que otro se aproveche de ella, será castigado con tres meses de prisión a tres años de penitenciaría

Aquí también el bien jurídico protegido es la propiedad. La norma busca extender el hurto común a este nuevo tipo de bien, que es el bien informático.

Artículo 5º. Dolo a través de los medios de comunicación. El que utilizando el correo, el teléfono, el fax, las fibras ópticas, la Internet o el E-mail, u otro medio de comunicación o telecomunicación similar, existente o a crearse, se procurare a sí mismo o a un tercero un beneficio patrimonial indebido, ya sea a través del fraude, el hurto, la malversación de fondos, el lavado de dinero, el soborno, el sabotaje, el espionaje, la conspiración, la extorsión, la difusión de material pornográfico, del ataque a la propiedad privada y el derecho a la privacidad de las personas, y otras figuras delictivas similares existentes o a crearse, será castigado con la pena correspondiente a cada uno de esos delitos, aumentada en un tercio

Con este delito se pretende evitar que los medios de comunicación sean utilizados por inescrupulosos, con fines dolosos e ilícitos. Es importante la previsión que abarca no sólo los medios existentes, sino también los “ha crearse”, ya que la dificultad en legislar sobre este tipo de delitos es la velocidad con que los mismos van cambiando, al mismo ritmo en que cambia la herramienta informática y las posibilidades que brinda.

Artículo 6º. (Tentativa). Con la excepción del artículo previsto en el artículo 2º de la presente ley (acceso culposo), los demás delitos podrán ser incriminados en grado de tentativa. En tal caso, las penas respectivas se reducirán de un tercio a la mitad

No se da posibilidad de tentativa cuando el delito es culposo.

Artículo 7º. (Agravante). Constituye una agravante especial el hecho de que los delitos previstos en la presente ley sean cometidos por funcionario público en ejercicio de sus funciones, o que el objeto del delito recaiga sobre sistemas de computación, software o soportes lógicos de cualquier entidad estatal.

El funcionario público es definido en el artículo 175 del Código Penal.

Artículo 8º. A los autores y cómplices se les aplicarán las penas de los artículos 88 y 89 del Código Penal.

Artículo 9º. Comuníquese, etc.

IX. Conclusiones.

1. Los delitos informáticos constituyen una nueva forma de delinquir que debe ser regulada.
2. Los sujetos, tanto activo como pasivo, tienen características propias y determinables.
3. Si bien en nuestro país la criminalidad en este aspecto es escasa, es necesario legislar en materia de delitos informáticos, el proyecto presentado en la legislatura pasada es un muy interesante punto de partida.
4. Al legislar debemos tener presente las soluciones adoptadas por otros países, a los efectos de que exista armonía en la regulación a nivel internacional. Esto es de suma importancia a los efectos de solicitar la extradición.
5. Es importante, no solo legislar a los efectos de tipificar los delitos, sino también crear una policía especializada, que sea capaz de identificar al sujeto activo frente a ilegalidades y reunir pruebas suficientes para lograr su condena.
6. Si el mundo digital ha sido un caldo de cultivo para este tipo de delincuencia, el cibereespacio lo es más, y la importancia del tema crece vertiginosamente y en relación directa con el desarrollo de Internet. Estar detenidos no es equivalente a no avanzar, es equivalente a retroceder.

[1] Jijena Leiva, Renato Javier: “La Criminalidad Informática”: Situación de Lege Data y Lege Ferenda en Chile”. Actas de III Congreso Iberoamericano de Informática y Derecho”. Mérida, España.

[2] Correa. “Derecho informático”. Depalma.

[3] Bergstein, Nahum. “Derecho penal e informática”. LJU tomo CXI, año 1995.

[4] Pacheco Klein, Jorge. "Introducción a los delitos informáticos en el ciberespacio. Normas y Jurisprudencia comentadas".

[5] Guibourg, Ricardo. “Manual de informática jurídica”. Astrea.

[6] Levene, Ricardo y Chiavalloti,Alicia. "Delitos Informáticos". VI Congreso Iberoamericano de Derecho e informática.

[7] Levene, Ricardo y Chiavalloti,Alicia. "Delitos Informáticos". VI Congreso Iberoamericano de Derecho e informática.