Tras los pasos de la Seguridad perdida. Delitos Informáticos

GUILLERMO CONSENTINO
JOSE ALBERTO GARCIA
DANIEL OMAR TEJERO
NESTOR FABIAN TEJERO

Universidad de San Juan Bosco de la Patagonia (ARGENTINA)

PROLOGO

Cuando en nuestras relaciones cotidianas observamos con agobiante malestar que la inseguridad se ha instalado en todos los niveles de nuestra sociedad y el hecho de que un mundo nuevo emerge a través de la informática, nos da la idea que en algunos aspectos lograremos, al menos como un anhelo, el restablecimiento de esa tan vapuleada seguridad.

¿En virtud de qué manifestamos o se nos representa espontáneamente ello?. Creemos que la generación y utilización social de nuevos conocimientos, artes y técnicas ha implicado, conforme indica la experiencia histórica, transformaciones culturales en las actividades productivas y, consecuentemente, en las formas de relación y organización social.

Los problemas que las innovaciones tecnológicas introducen en la sociedad, conforman una temática que, considerada desde una perspectiva político-criminal, entendida como modelo de orientación para el derecho penal futuro y marco de interpretación de la dogmática del orden jurídico-penal vigente, permiten señalar la existencia de dos aspectos básicos, constituídos por:

- Los efectos de la concentración económica;

- La necesidad de que los elementos típicos (descriptivos y normativos) se expresen a los efectos de respetar los principios de legalidad y tipicidad, en tipos

que -en tanto descripción de la conducta prohibida por la norma- permitan realizar la adecuación típica de las acciones prohibidas con precisión.

Concentración económica: la tendencia a la concentración económica, expresada por medio del accionar de empresas multinacionales, pone de relieve la contradicción de intereses entre países con distintos niveles de desarrollo. La evolución del comercio mundial evidencia una creciente especialización intra-tecnológico-industrial entre los países desarrollados y en desarrollo, en lo que respecta al comercio de manufacturas, servicios y tecnologías.

En este plano se comprueba la presencia de una criminalidad, no reprimida penalmente, que, asentada en el abuso del poder económico y político, trasciende con su actuación los límites geográficos de los Estados, afectando los intereses y derechos económicos de los países en desarrollo.

Sobre esta situación el profesor Tiedemann ha señalado que "las investigaciones criminológicas más recientes, especialmente en los países angloamericanos y escandinavos, han demostrado, en base a estudios sobre la génesis normativa, que la no tipificación de ciertas conductas puede deberse a la influencia ejercida sobre los órganos legislativos por poderosos grupos de personas interesadas. En dichas situaciones, quien tiene ese poder se encuentra jurídicamente (por encima del alcance de la ley) -para utilizar una expresión acuñada en el VI Congreso de las Naciones Unidas sobre Prevención del delito y tratamiento del delincuente (Caracas, 1980)- en relación con el abuso del poder, especialmente por parte de las empresas multinacionales o transnacionales".

Cuestiones de tipicidad: la técnica ha constituído también, en forma tradicional, un instrumento y objeto de acciones que afectan intereses que la comunidad procura tutelar. En este sentido, la experiencia indica que la utilización de nuevas modalidades delictivas suelen anticiparse a las previsiones penales, que aparecen así como desactualizadas, imposibilitadas de operar como mecanismo de prevención general -impidiendo que la pena opere como inhibidor de ciertos comportamientos frente a la sociedad- o de represión penal de conductas.

Sin embargo, como indica el profesor Zaffaroni, el nivel de riesgo social derivado de situaciones como la contaminación ambiental, el despliegue nuclear, el volumen financiero de la transferencia electrónica de fondos y la centralización de datos personales, por mencionar algunos aspectos del problema, obliga a acentuar los trabajos interdisciplinarios a los efectos de poder establecer un

sistema de prevención eficiente, que avance sobre el desfase normativo y el recurrente criterio de pretender resolver cualquier tipo de conflicto social mediante formulaciones típico-penales abiertas, que independientemente de atentar contra la seguridad jurídica, sólo contribuyen a evidenciar, más allá de la existencia de una referencia legal, la ineficacia del sistema de justicia penal en estos supuestos.

Efectuado este escueto análisis, sobre lo que creemos la implantación del problema de la inseguridad en que actualmente vivimos, podemos afirmar a modo de hipótesis que la instauración de la Informática en los distintos niveles de nuestra sociedad nos llevará a reencontrarnos con la seguridad social, económica, política, educacional, judicial, etc.

Es nuestro agradecimiento a esta cátedra que nos permite investigar un tema tan profundo y lleno de controversias, lo que nos llevó a efectuar esta investigación y ofrecer nuestro humilde aporte, plasmado en esta monografía.

EVOLUCION Y REPERCUSIONES SOCIALES DE LA INFORMATICA

La informática, o sea la "ciencia del tratamiento lógico y automático de la información mediante ordenador", tuvo, como es sabido, en los últimos años, sobre todo tras la aparición de la telemática y los microordenadores, un desarrollo enorme y desempeña hoy un papel extremadamente importante en el campo social y económico, tanto a nivel individual como colectivo.

En verdad, faltan datos precisos y unívocos acerca del número de ordenadores que funcionan actualmente en todo el mundo, si bien la proliferación de sistemas cada vez más sofisticados y complejos es tanta, que existe el temor de que se forme una verdadera "telaraña informática" en torno al individuo y a la sociedad misma.

A los efectos de una primera orientación, las áreas afectadas por la informatización pueden dividirse en: sector del registro civil, fiscal, de la previsión social, judicial y policial, de la educación y la instrucción, de la defensa nacional, comercial y bancario, de los transportes y seguros, y de las organizaciones profesionales.

ACTUALIDAD DE LOS BIENES INCORPORALES

Materia objeto de examen: en lo que concierne a las cosas materiales, muebles o inmuebles, es respecto de ellas que se ha desenvuelto principalmente la doctrina y la jurisprudencia. Y, comprendidos en la concepción amplia del vocablo "propiedad" los bienes inmateriales, la propiedad intelectual e industrial.

Es decir, no es que los bienes inmateriales o incorporales no hayan sido considerados en la esfera de los derechos patrimoniales, pero es también cierto que ha sido en las últimas décadas que su importancia acreció, exigiendo su examen más detenido.

Ello así, porque el avance de la ciencia y de la técnica ha producido distintas manifestaciones y logros, a los que según algunas orientaciones son aplicables las reglamentaciones de las mencionadas propiedades, intelectual o industrial, o bien son necesarias nuevas reglamentaciones jurídicas que permitan acompañar el progreso experimentado.

Preexistencia y continuidad de la calificación de los bienes incorporales o inmateriales: según la sucinta relación antecedente, es apreciable que los bienes inmateriales o incorporales no estaban excluidos en el cuadro de los derechos patrimoniales.

Ya tales bienes estaban definidos en el derecho romano, puestos de relieve en la obra de Ginossar, en la cual desarrolla su concepción sobre una nueva clasificación de los derechos patrimoniales.

En lo pertinente, adecuado a nuestro tema, resumiendo su idea, creemos que los romanos, guiados por su admirable instinto jurídico, consideraron que la propiedad difiere de los demás derechos, pues ella absorbe el bien sobre el cual recae, por lo que resulta lógico colocar en un mismo pie entre las cosas que forman el activo de un patrimonio de una parte, las cosas corporales (tierras, esclavos, ropas, oro, plata, etc.); y de otra parte, las cosas incorporales, es decir, los derechos, especialmente las obligaciones, y los derechos de obligación de crédito.

Aubry y Rau sustentaron que "el término propiedad ha sido extendido a las cosas incorporales y comprendido en él a la propiedad literaria, artística e industrial".

En este orden de consideraciones, en la obra de Planiol-Ripert se advierte una denominación significativa de los derechos sobre las cosas incorporales, pues se los designa como propiedades incorporales.

Si recordamos la proposición de Ginossar respecto de una nueva clasificación de los derechos patrimoniales y tenemos presente el concepto de Savatier de que "todo derecho, aún sobre una cosa concreta es incorporal, no existiendo sino bienes incorporales", estimamos que ellos encierran principios jurídicos que permiten zafar la caracterización del derecho de propiedad tal como se lo limita a las cosas corporales o materiales.

Derecho comparado: En los códigos y en las legislaciones latinoamericanas y europeas, los derechos de autor o de inventor están caracterizados como derechos de propiedad o como derechos de autor o de inventor.

Valdés Otero expone -en relación con la ley del Uruguay- su criterio favorable a la denominación de "derechos de autor", incorporada por el legislador a la ley respectiva.

"Creemos -sostiene- ajustada la denominación de derechos de autor que ha recibido nuestra ley, pues, a diferencia de los derechos intelectuales, que también se encuentra ampliamente difundida en el derecho comparado, no compromete una definición en el problema de la naturaleza jurídica. En la doctrina brasileña se sostiene que el derecho de autor es una propiedad inmaterial.

Rojina Villegas, en la doctrina mejicana, estima que "queda definida la naturaleza de este derecho de autor o propiedad intelectual, resolviendo como primer punto, que se trata de un derecho real, y no personal. Es decir, que se trata de un derecho patrimonial de naturaleza real.

Estima Puig Brutau que el calificativo de propiedades intelectuales e industriales constituye un recurso del razonamiento jurídico para encajar determinados intereses en el sector jurídico donde podían hallar protección, cual es el de los derechos de propiedad; asimismo, que en la reelaboración doctrinal, "el calificativo -expresa- queda a veces sustituido por el de propiedad sobre bienes inmateriales. La perduración del concepto de propiedad garantiza la continuidad de unos efectos, y el nuevo calificativo señala el hecho indudable de que la equiparación es sumamente artificiosa".

Proyección de las formulaciones precedentes: los derechos del autor y del inventor quedan, pues, encuadrados en el concepto de "propiedad", sobre la base de su extensión a los bienes, cosas corporales o materiales, independientemente de la necesidad de determinación de la naturaleza jurídica de los bienes inmateriales.

Estimamos que prevalece la noción de derecho independientemente de la corporeidad o incorporeidad del resultado de la creación o de la actividad inventiva. En cuanto a la conservación de la expresión "propiedad intelectual", estimamos que se subordina a los preceptos constitucionales según que ellos determinen o no ese concepto.

Pero ello no empece a sustentar la expresión de derechos intelectuales o industriales, cuyo objeto puede ser todo cuanto puede resultar de la creación del hombre (patentes de invención, marcas, modelos de utilidad, know-how, software y productos obtenidos por esos procedimientos) reconocidos como derecho subjetivo por el ordenamiento normativo.

RELACIONES ENTRE LA TECNOLOGIA Y EL DERECHO

Las innovaciones y las invenciones técnicas han sugerido la creación de nuevos derechos, y, a menudo, de derechos específicos. En ciertos casos, se impuso al Legislador la necesidad de una nueva reglamentación; así ocurrió con la invención del automóvil, que impuso una cantidad de normas de policía y de circulación, codificadas hoy en día en un "código de la circulación".

Hasta ahora, sin embargo, las relaciones entre la informática y las reglas del derecho son ambiguas.

Sea como fuere, desde hace ya un tiempo se viene hablando, en varios países -sobre todo en Alemania, España, Estados Unidos, Francia y Noruega-, de un "derecho de la informática", definido recientemente como "conjunto de las normas, de las instituciones y de los principios aplicables a los hechos, actos y actividades relacionadas con el tratamiento de la información y con la informática". Se trataría, de un "derecho especial en marcha hacia la autonomía".

Según algunos autores, el derecho de la informática derivaría su unidad de la originalidad técnica caracterizada por el fenómeno informático, por el cual, en muchos casos, las soluciones jurídicas tradicionales resultan inadecuadas.

En opinión de otros, el derecho de la informática será esencialmente un punto de cruce entre diversos derechos, pues la técnica de los ordenadores repercute en numerosas ramas del derecho: del derecho civil al derecho comercial y al derecho de autor; del derecho constitucional y administrativo al derecho penal.

EL DERECHO PENAL DE LA INFORMATICA

Si se acepta esta interpretación en lo concerniente a la multidisciplinariedad del derecho de la informática, podría hablarse entonces de un "derecho civil de la informática" que debería regir especialmente las cuestiones que surgieren del uso y de la producción de programas y contratos informáticos; de un "derecho público de la informática", que reglamentaría sus rasgos constitucionalistas y administrativos; y de un "derecho penal de la informática", cuyas funciones serían las de prever y reprimir específicamente las violaciones típicas del propio sector.

En sentido general el derecho penal de la informática sería esa subespecie del derecho de la informática que respecta a los actos ilícitos de índole penal como quiera vinculados con el empleo del ordenador. En sentido estricto, el derecho penal de la informática podría ser definido como aquel grupo de normas jurídicas por las cuales el Estado, prohibe, con la amenaza de una pena, ciertos comportamientos humanos específicos en el campo de la informática.

La creación de un derecho penal de la informática presenta, empero, dificultades de no poca cuenta, y sea desde el punto de vista científico-dogmático o desde el del derecho positivo. En efecto, han de proceder a formular normas específicas, modificar eventualmente el sistema de sanciones, coordinar las distintas normas entre sí; todo ello teniendo en cuenta principios fundamentales vigentes en los sistemas jurídicos de los países occidentales, que generalmente prohiben el recurso a la analogía en materia penal y están basados en el principio de legalidad estricta.

AFECTACIONES AL SOFTWARE. PROPIEDAD INTELECTUAL

Se ha definido al software como "el conjunto de datos e instituciones destinadas a producir información, que permiten controlar el funcionamiento del hardware y lo habilitan para cumplir determinados resultados", comprendiéndose

dentro de ese concepto, los programas de computación, su descripción y la documentación complementaria.

La detección de distintas conductas que implican usar sin autorización, modificar, borrar o copiar datos, informaciones o programas, plantea la necesidad de establecer, en atención al carácter inmaterial del objeto, cuál es el marco de protección jurídico-penal del software.

Al respecto existen dos posturas según entiendan que el soporte lógico (software) de los sistemas automáticos de procesamiento de datos se halla protegido por las normas que tutelan los derechos del autor (copyright), o bien se entienda que este marco legal resulta limitado e inadecuado a estos efectos.

Una corriente opina que el resguardo está brindado por las normas del derecho autoral, sosteniendo la viabilidad de proteger los "derechos de propiedad intelectual" sobre los programas de computación, ya que éstos constituirían una "creación personal intelectual".

Desde otra perspectiva se ha sostenido que el destinatario de las "obras" protegidas por el derecho de autor es el hombre, mientras que los programas de computación -fundados en un algoritmo- son un conjunto de instrucciones, que no revelan la personalidad del programador, destinadas a una computadora, y no a la percepción humana.

PROTECCION JURIDICA DEL "SOFTWARE" Y DE LOS MICROORGANISMOS

En nuestra legislación no están reglamentados los bienes incorporales mencionados supra, el "software" y los "microorganismos".

En el derecho comparado prevalece la orientación según la cual a los programas del computador le son aplicables las leyes de propiedad intelectual. En cuanto a los microorganismos, en la doctrina, jurisprudencia y convenios internacionales, son considerados patentables.

Desde el punto de vista legislativo no es de buena técnica establecer definiciones en las normas en que se perceptúen los derechos, así como hallar puntos de partida inconmovibles o definir la naturaleza jurídica a partir de todo lo cual sea dable su clasificación y sistematización.

En estos casos, se está en presencia de un hecho nuevo en el campo de la creación y de la técnica, con bases en proyecciones que la ley de propiedad intelectual no previó ni pudo prever.

Objetivamente considerada, la concepción del programa en la medida que su significado y aporte representen un interés es susceptible de protección jurídica, admitido que todo derecho, en el criterio de Jhering, "...establece la expresión de un interés reconocido por el legislador que requiere y merece protección...". Los derechos se transforman, por lo tanto -prosigue-, en la medida que cambian los intereses de la vida...".

La ley 11723 (Ley de Propiedad Intelectual) no sólo reconoce derechos a las obras extranjeras, sino que nuestro país se ha adherido a los convenios internacionales de protección del derecho de autor (Convención Universal sobre derecho autor y Convención de Berna), que contienen preceptos concordantes que permiten asegurar en todos los países la protección del derecho de autor.

En su consecuencia se operaría la protección del "software", sin demoras en la extensión de los convenios internacionales y sin disposiciones restrictivas, pues como acontece en nuestro país, no existe ley que los reglamente.

En consecuencia de lo expresado es fundamental la sanción de una ley especial, que necesariamente debería establecer: el objeto protegido debe contemplar los programas descritos en forma inteligible, de manera tal que pueda facilitar el uso y aplicación del software, el "originario" y el "derivado", así como la adaptación, reproducción o innovaciones de que pueda ser objeto.

La protección debería, asimismo, extenderse a los "algoritmos" y a la "combinación de algoritmos" aún conocidos.

Con las precisiones correspondientes y normas que integren los principios formulados, es dable evitar no sólo la monopolización de los registros, sino también obtener la consecuencia esencial, cual es el logro de un desarrollo propio en la materia, pues si el objeto de la protección es amplio, mayor será la posibilidad de registro de innovaciones, perfeccionamientos y de combinaciones de "algoritmos", aún conocidos.

En este punto cabe reglar los casos de software no registrados, como así también la responsabilidad civil y penal por la violación del derecho acordado.

Para ello es necesario reglamentar principalmente que la obligación de otorgar licencia, no se frustre por recursos dilatorios y excusas del titular, mediante las cuales pretenda justificar la falta de comercialización, reproducción o uso del software. O pretensión de justificación mediante la importación. En el punto debería contemplarse la hipótesis de nulidad del registro.

En cuanto a la patentabilidad de los microorganismos, el régimen que reglamenta el reconocimiento internacional del depósito de microorganismos a los fines del procedimiento en materia de patentes, se rige por el Tratado de Budapest de 1977.

El Tratado establece como principal característica, que un Estado contratante que permita o exija el depósito de microorganismos, a los fines del procedimiento en materia de patentes, debe reconocer, para ese procedimiento, el depósito de un microorganismo efectuado ante una autoridad internacional de depósito, lo mismo si esa autoridad está establecida en su territorio o fuera de él. En otras palabras, basta un sólo depósito hecho a una autoridad internacional de depósito única a los fines del procedimiento en materia de patentes ante las oficinas de patentes de todos los Estados contratantes y ante una oficina regional de patentes, si ésta declara que reconoce los efectos del tratado.

HACIA LA DELINCUENCIA INFORMATICA

Esta proyección de la tecnología informática expresada por la cantidad de ordenadores en funcionamiento, en las más diversas tareas socialmente útiles, ha generado, asimismo, un conjunto de conductas, relacionadas con la operatoria de los sistemas automáticos de procesamiento de datos, que son aptas para originar perjuicios de distinto orden, como las lesiones a la intimidad, la seguridad, (político-industrial), o al patrimonio.

La acumulación, archivo, y centralización de datos, en bancos automatizados, con sus posibilidades de asociación, combinación, devolución y divulgación, genera una situación que ante el acceso, modificación, destrucción o difusión no autorizados de estos datos (referidos, por ejemplo a profesión religiosa, actividad política, situación económica, salud, empleo), puede significar perjuicios en la esfera privada de los individuos. La protección de la intimidad y

de los datos personales ha originado un gran movimiento, a nivel internacional, como asimismo dentro de distintos países, expresados en los proyectos elaborados en el seno de la Comisión Económica Europea, el Consejo de Europa y la O.S.E.D.E., a los efectos de establecer instrumentos que permitan tutelar al individuo, ante los riesgos derivados del uso no autorizado de la información contenida en los bancos automatizado de datos. Se procura establecer previsiones respecto a la difusión de datos personales, el acceso a ellos por personas no autorizadas, con posibilidades de control y rectificación de datos por parte de los interesados.

Las posibilidades de vulnerabilidad de los sistemas informáticos han quedado evidenciadas en casos como el registrado en el año mil novecientos ochenta y ocho, cuando un grupo de "hackers" de Alemania Occidental, ingresó y operó por medio de las líneas telefónicas internacionales en las computadoras de la Nasa, lo cual demandó ulteriormente meses de trabajo a los efectos de proceder a cambiar los passwords y limpiar las trampas (trap doors) que los intrusos habrían colocado para poder tener acceso al sistema.

En el plano de los intereses económicos, las entidades bancarias, compañías de seguros y empresas productoras de bienes y servicios en general, pueden resultar damnificadas, con importantes perjuicios patrimoniales. En este aspecto, también se puede referir un caso, detectado en junio de mil novecientos ochenta y ocho, cuando operadores no autorizados, mediante una intervención en el programa, giraron la suma de cincuenta y cuatro millones de dólares de un banco suizo a otra entidad financiera para su cobro.

La información objetiva disponible permite establecer proyectivamente que el incremento de la informatización en las operaciones financieras determinará que los delitos contra el patrimonio adquieran una progresión desconocida hasta el presente, y que el mayor volumen de afectaciones económicas se concentre en el futuro en este tipo de operatoria.

En este área las tareas de investigación de campo, a partir del análisis de casos sometidos a investigación judicial, se ve dificultada por la tendencia a no denunciar este tipo de hechos, por parte de los damnificados. Se considera que esta actitud reticente se debe a que las empresas perjudicadas procuran evitar poner en evidencia que sus sistemas informáticos son vulnerables, por el efecto desfavorable que el conocimiento de esta circunstancia podría tener sobre sus clientes.

Las conductas perjudiciales cometidas en relación con los sistemas informáticos pueden ser realizadas, básicamente, con dos modalidades: como manipulaciones o usos del programa, utilizando equipos automáticos de procesamiento de datos (por ej: confección de balances falsos, administración fraudulenta), donde el sistema informático es el medio de la acción, o bien acciones que tienen el sistema como objeto (por ej: hurto del soporte físico, daño en las instalaciones, robo del hardware), supuestos que no constituyen una criminalidad diferenciada y se adecuan a los tipos penales clásicos, vigentes en el ordenamiento positivo.

Desde esa perspectiva los supuestos específicos de delincuencia informática, conforme a la experiencia internacional, estarían básicamente constituidos por los siguientes casos:

- uso no autorizado del ordenador o sus equipos, ya sea excediendo el límite de la autorización para operar, ya sea introduciéndose en el sistema;

- introducción, alteración, modificación, utilización, copia o destrucción, no autorizados, de datos, sin remoción de soporte magnético;

- violación del secreto informático;

- intervenciones en el programa a los efectos de posibilitar transferencias electrónicas de fondos con afectaciones al derecho de propiedad.

LEGISLACION ARGENTINA A ESTE RESPECTO

La legislación argentina sobre propiedad intelectual expresada en la ley ll723, en los arts. 7l y 72, establece distintas formas de defraudación de los derechos de propiedad intelectual, y sobre la obra, remitiendo, a los efectos punitivos, a las penalidades previstas para el delito de Estafa (art. l72 del Código Penal Argentino), que prescribe para este ilícito pena de prisión de uno a seis años.

Para que proceda entonces la adecuación de la acción defraudadora a la descripción del tipo, debe verificarse la concurrencia de un comportamiento doloso y los elementos del tipo objetivo de estafa (engaño, error, disposición patrimonial, perjuicio).

De la descripción contenida en el art. 72 de la ley ll723, surge que el objeto de protección está constituido por la "obra" lo que nos lleva a señalar dos cuestiones:

a) se efectúa una remisión a otras disposiciones de la ley ll723, a los efectos de poder establecer qué se entiende por "obra", lo cual nos coloca ante un tipo de disposición que la dogmática penal califica como "ley penal en blanco", denominándose de esta manera a las leyes que "sólo contienen la conminación punitiva y que respecto del tipo se remiten a otras normas", y

b) se plantea el tema de precisar si el software puede ser considerado como una "obra", en el sentido que la entiende la ley de propiedad intelectual. Sobre esta cuestión ampliamente debatida, existirían limitaciones en cuanto poder considerar el elemento básico del software: el algoritmo (procedimiento de cálculo constituido por secuencias de operaciones numéricas-lógicas), como asimismo, al "código objeto" o "programa objeto" (transformación del "programa-fuente" en un programa sólo legible por la máquina y constituido por símbolos binarios), sobre el cual se efectúan generalmente las copias no autorizadas de software, como una "obra" -creación del intelecto humano-.

Por su parte, la referencia efectuada en el art. 7l al expresar que "será reprimido... el que de cualquier manera y en cualquier forma defraudare los derechos de propiedad intelectual que reconoce esta ley", reúne no sólo la referida característica de "ley penal en blanco" -cuando expresa: a "los derechos de

propiedad intelectual que reconoce esta ley"- sino que al señalar, además, "al que de cualquier manera y en cualquier forma defraudare", incurre en una descripción inespecífica, propias de los llamados "tipos abiertos", o sea, aquellos en los cuales existe un grado amplio de abstracción caracterizándose "por la circunstancia de que los elementos fundamentadores de la ilicitud del hecho no están totalmente enunciados en la ley". Esto obliga al juzgador a recurrir a pautas o reglas que están fuera del tipo penal para procurar resolver el conflicto sometido a su decisión.

De esta manera, ningún hecho, más allá del reproche social que pueda merecer, o el perjuicio que causare a la comunidad, puede ser merecedor de una pena del derecho penal, sino existe una ley previa que lo haya declarado punible. Este es un costo que la sociedad debe asumir en mérito a contar con un sistema jurídico seguro que conlleve a una interpretación precisa y estricta de la ley penal, a los efectos de evitar extenciones subjetivas que determinen la persecución de conductas no previstas en el tipo penal.

Consecuencia directa del principio de legalidad, adoptado por el art. 18 de la Constitución Nacional Argentina, es la prohibición de la analogía, entendida como la aplicación de la ley a un caso similar al legislado, pero no comprendido en su texto, en el ámbito del derecho penal, en perjuicio del imputado.

La sistemática de esta ley de propiedad intelectual, en los aspectos considerados, genera un marco técnico-legal incierto. Por lo cual entendemos, en atención a posibilitar criterios seguros en la aplicación de la ley penal, evitar interpretaciones analógicas y resguardar el principio constitucional de legalidad que corresponde proceder a legislar, en esta materia, en forma específica y subsidiaria, respecto de las normas del derecho privado, por parte del ordenamiento penal.

ENTRE EL HURTO Y LA ESTAFA. ÉSTA ES LA CUESTION

Resultaría importante destacar al respecto el trabajo realizado por Sandro F. Abraldes, publicado en la revista "La Ley", con la finalidad de demostrar que en todos los supuestos en que se obtenga un desplazamiento patrimonial indebido a través de un medio mecanizado o informatizado, constituye lisa y llanamente el delito de Estafa.

Comienza realizando una distinción entre los delitos de Estafa y Hurto, determinando que en el primero de los casos se está en presencia del engaño y la perfidia. En la Estafa se da a la mentira la apariencia de verdad. Su fin es la defraudación por el abuso de confianza.

Dice que conforme lo determina Creus, en la defraudación, la acción de la víctima se origina en su voluntad viciada por un error suscitado en ella, como también puede ocurrir que ese error induzca a la víctima a omitir conductas, cuyas omisiones facilitan la actividad ilícita del sujeto activo.

Otra diferencia está dada por el objeto de la acción, desde que objeto del hurto sólo puede ser la propiedad en su sentido de tenencia de cosas muebles, y en la usurpación de inmuebles, ese objeto sólo puede ser, su tenencia o posesión o la cuasi-posesión de los derechos reales, la estafa puede recaer sobre cualquiera de los contenidos posibles de la propiedad, como la tenencia o la posesión de una cosa mueble o su dominio, las ventajas económicas correspondientes a una explotación comercial o la indemnización pertinente a su frustración, el beneficio jubilatorio, la garantía susceptible de valor pecuniario que significa un embargo, el valor de un crédito, etc.

El autor coincide con Mancini en que el objeto específico de la tutela penal es el interés público en la inviolabilidad del patrimonio, que el Estado pretende proteger contra las acciones fraudulentas tendentes a arrancar prestaciones útiles con provecho propio o ajeno. Con la incriminación de la estafa la ley penal considera genérica y objetivamente el patrimonio y lo tutela con un fin objetivo y colectivo, dejando a la ley civil la protección de los distintos derechos subjetivos.

En el tema en cuestión resulta claro que la protección penal que brinda el delito de estafa es, a la par que distinta, mucho más amplia que la de hurto. Esta amplitud otorga al Juez una herramienta más idónea a la hora de individualizar la pena, con lo que la holgada gama de casos que ofrece la realidad, será siempre mejor cubierta por el delito de estafa que por el de hurto. La expectativa social de penalización y la esencia retributiva de la pena son aspectos que la estafa contempla de mejor manera en estos supuestos.

En la doctrina nacional, la corriente mayoritaria que encuentra su mayor exponente en Soler afirma que "sin error no hay estafa", así como no la hay sin ardid aún cuando mediante alguna maniobra se logre un beneficio indebido. El

que mediante una moneda falsa logra sacar de un aparato automático el artículo que contiene no comete estafa sino hurto ya que si bien existe maniobra no existe ninguna mente errada. No así cuando han existido maniobras sobre medidores de luz o de gas, para determinar un error en la factura sobre la base de falsas cifras.

El autor también opina que en un caso en que el sujeto trató de obtener dinero ajeno mediante la utilización de una tarjeta magnética también ajena y sin autorización, ignorando el número de clave que correspondía, ese comportamiento se entendió como constitutivo de hurto en grado de tentativa.

También Creus se enrola en esta alternativa, para quien la maniobra de fraude tiene que determinar el error de la persona, si por ejemplo, aquella tiende a equivocar los controles de una máquina expendedora para que acuse más de lo debido, no hay estafa sino hurto, pero ello no ocurre cuando la alteración de la máquina es el medio al que se acude para engañar a la persona que la emplea para controlar la medida de la prestación que debe realizar.

Donna en disidencia sostiene que no existe estafa en este caso sino hurto, por que el error que lleva la lectura del medidor no es determinante de la entrega del gas o de la electricidad, sino que es representativo de su valor a posteriori.

Rojas Pellerano sostiene que el ardid o engaño empleado mediante aparatos mecánicos constituye estafa. El hurto es la excepción. Fundamenta su posición en la "objetividad jurídica" pues la falsedad o engaño ofende la relación a formarse y en vía de ejecución (sea un contrato civil, comercial o administrativo).

Esta tendencia extrema de considerar configurada una estafa en todas las posibilidades aludidas encuentra algunos escasos precedentes en nuestra jurisprudencia, siendo uno de ellos el adoptado por la Cámara de Apelaciones de la Capital Federal, que consideró que la introducción de un disco de metal en lugar de una moneda en el molinete del tranvía subterráneo para eludir el pago constituye el delito de estafa si advertida la maniobra el actor fue detenido en el acto.

En la doctrina Italiana Tolomei sostiene que en las maniobras realizadas sobre aparatos automáticos distribuidores de mercancías existe estafa. Estos aparatos proporcionan un bien contra el pago de un precio por lo tanto el que simula el pago del precio engaña al propietario del aparato. Entiende que la

función de estos aparatos equivale a la que cumple un mozo que entrega comida a precio fijo, y así como comete estafa quien entrega al mozo una moneda falsa, también existe estafa cuando el fraude se realiza sobre un distribuidor automático.

En la doctrina Española existe un criterio dominante que niega la aplicabilidad del delito de estafa sosteniendo que a las máquinas no se las puede engañar y que en estos casos la sustracción se lleva a cabo de una manera subrepticia aunque astuta sin previa entrega ni voluntad humana directamente operante por parte del engañado no presente, por lo que concluyen remitiéndose a la figura de hurto.

En la corriente opuesta, la posición de Bajo Fernandez, no duda en calificar como estafa la conducta de quien obtiene dinero del cajero automático de un banco utilizando una tarjeta robada o hallada u otro objeto que la sustituya.

Análogo temperamento propicia Bustos Ramirez, ya que, a pesar de la amplitud de la defraudación y de la estafa en su pretensión de abarcar medios intelectuales de ataque al patrimonio, se ha producido un desfasamiento con la realidad, en razón del gran avance tecnológico producido. Así las cosas, el surgimiento de la computarización y maquinización de las actividades económicas ha traído como consecuencia la utilización de nuevos medios que no se pueden incluir dentro de las defraudaciones o estafas en virtud del principio de legalidad, como por ejemplo, el sujeto que se logra conectar con el ordenador de un banco y que a través de la alteración de su programa consigue que le sean borradas sus deudas, ha realizado una actividad que no se puede incluir en la estafa ni en ningún otro delito contra el patrimonio.

El fallo plenario "Ruzzolino, J. L." del año 1961, se reunió para resolver en qué disposición legal encuadrar la conducta de quien mediante la utilización maliciosa del conducto por el que se recuperan las monedas de un teléfono público, retira en su provecho las que quedaron depositadas por no haberse obtenido la prestación del servicio. El voto de la mayoría sostuvo que trasladado el concepto de estafa al ejemplo del plenario se advierte enseguida la ausencia de esa relación causal entre engaño, error y disposición.

La postura contraria sostuvo que ninguna dificultad existiría si en razón de hallarse el aparato efectivamente descompuesto, por tal motivo no recupera la moneda y después un tercero valiéndose de cualquier treta, que no importe forzar la cosa de donde ha quedado retenida, la sustrae para sí, pues tal apoderamiento

importa el delito de hurto simple... pero no ocurre lo mismo si la maniobra ha sido antes preparada a los fines de hacer creer al usuario que aquella posibilidad de rescate deriva de algún defecto propio de la máquina induciéndose de esa manera a su abandono equivalente en los hechos a una práctica entrega. Por lo que tal conducta resultaría una típica acción estafadora por un medio mecánico tan eficaz e idóneo al efecto como cualquier otro ardid o engaño de índole personal.

El autor del artículo continúa refiriéndose respecto de la inaplicabilidad del tipo penal de hurto por cuanto el mismo exige que exista la acción de "apoderarse" en el sentido de aprehensión física, material de la cosa por lo que aparecen grandes dificultades a la hora de proyectar las manipulaciones fraudulentas, mediante medios mecánicos, automatizados o informatizados, en la mencionada conducta típica, debiendo también tenerse en cuenta la dificultad de asignarle el carácter de cosa mueble al dinero contable, escritural o documental.

Hace también referencia a la dificultad de calificar como estafa los delitos cometidos a través de medios informatizados en los que opere una persona humana, en virtud de la ya comentada inexistencia de una mente errada.

No obstante ello este autor se inclina por encuadrar estas conductas en el artículo 172 del código penal y ejemplifica diciendo que si un consumidor accede a una máquina para obtener un bien, entabla una relación con la persona física o jurídica, que valiéndose del referido medio, entrega el bien. Sería desatinado reconocerle a un simple aparato el dominio de un acto de disposición patrimonial.

Regresando al caso de quien con una tarjeta extrae antijurídicamente fondos de un cajero automático, Nuñez diría que el mecanismo ya no expresa la voluntad de aquel que condicionó el acto de disposición a la forma legítima de su funcionamiento. ¿por qué no sostener que el cajero sigue expresando aquella voluntad preordenada pero sobre la base de un engaño, tal como no dudaría en afirmar Tolomei, cuando seguramente, equipararía este supuesto al del mozo que se le da una moneda falsa?. Es evidente que según esta línea que el acto ejecutivo es realizado a consecuencia del engaño de que es objeto el elemento intelectivo pre-establecido. Así puede aseverarse que el sujeto tiene el dominio mediato de la disposición patrimonial que lo perjudica.

Desde el principio fue intención del trabajo de este autor situar dogmáticamente a estos comportamientos en el art. 172 del Código Penal, Para ello ha demostrado lo siguiente:

- respecto al engaño, es imprescindible aceptar que el falseamiento de la realidad que él implica, no comporta necesariamente una relación directa y personal entre dos seres humanos, lo que debe ser desechado por vía de interpretación solamente comprensible en otro contexto histórico.

- Sobre el error, debe negarse su condición de elemento autónomo del tipo objetivo, circunscribiendo su función a la delimitación restrictiva del engaño típico, por lo que siguiendo una interpretación de esta índole quedan suprimidos algunos de los obstáculos que alguna doctrina invoca para calificar de estafa a las defraudaciones mediante medios mecanizados.

Ha probado, desde varias posiciones, que en lo concerniente al acto de disposición, debe aceptarse que se pueden realizar disposiciones materiales con el auxilio de una máquina, y que la colaboración en el traspaso patrimonial lesivo que este elemento implica, puede atribuirse a la persona física, pues el dominio de la disposición, sin duda, le corresponde.

Aún siendo evidente que la figura de estafa no fue concebida para esta nueva manifestación de la criminalidad defraudatoria, su aplicación en este ámbito cabe, sin contradecir las exigencias del principio de legalidad.

Esta nueva gama de delitos que estudiamos, no solamente han provocado inconvenientes y preocupaciones a la legislación penal argentina, sino también a países de notable desarrollo de Europa, tales como:

ALEMANIA

Donde el derecho penal ha tropezado con dificultades considerables, ya que en la década del ochenta, más precisamente del año mil novecientos ochenta y dos, se acepta la incorporación a la legislación penal de dos nuevos tipos penales, como el de "estafa por ordenador" y de "falsificación de datos almacenados", habiendo quedado resueltas las lagunas legales más importantes del Código Penal Alemán en relación con la lucha contra las manipulaciones del ordenador, permaneciendo abierta la cuestión de si, a causa del rápido desarrollo técnico

luego de esta aprobación podría considerarse que esté ya nuevamente anticuado, debido al constante crecimiento del sistema informático.

Los delitos informáticos más característicos en Alemania, y que han pasado a un primer plano resultan ser las manipulaciones de ordenadores, el espionaje informático, el hurto de software, el sabotaje de ordenadores, el hurto de tiempo, así como la comisión de delitos económicos en general por medio de ordenadores.

Manipulaciones del ordenador: consiste en modificaciones de datos, practicadas especialmente por empleados de las empresas perjudicadas con el fin de obtener un enriquecimiento personal. Se considera al ordenador como una instalación de procesos de datos, es decir, como una instalación en la que se introducen los datos que se tienen que procesar (el denominado input) y la forma de proceso deseada (a través del programa y los recursos de consola complementarios) obteniéndose automáticamente el resultado del proceso (el denominado output), se ponen de relieve los diversos métodos de manipulación del proceso de datos: el autor puede en un principio introducir datos falsos en el ordenador (manipulaciones del input), puede alterar el orden del proceso (manipulaciones del programa y de la consola), o bien puede posteriormente falsear el resultado, inicialmente correcto, obtenido del ordenador (manipulaciones del output).

Espionaje informático y hurto de software: el espionaje informático constituye en el ámbito de la criminalidad por ordenador la segunda forma más frecuente de delito. Para el autor es especialmente lucrativa, y para la empresa afectada es especialmente peligrosa, porque en los centros de cálculo de la mayoría de empresa con frecuencia se almacenan en muy poco espacio, importantes y numerosos secretos de las mismas.

La elevada capacidad de almacenamiento de datos que permiten los sistemas informáticos y la posibilidad de copiarlos rápida y discretamente con la ayuda del ordenador, conducen al hecho de que el espionaje informático abre nuevas dimensiones al espionaje económico.

En los últimos tiempos un punto central del espionaje informático y del hurto de software se observa ante todo en el ámbito de la concesión de licencias de programas, por ello en este ámbito se tendría que prestar atención al hecho de que los programas se transmitan solo en código objeto (no modificable), y que

contengan notas de bloqueo adecuadas (en especial las denominadas fechas de expiración y, si fuera posible, también bloqueos de copias).

Sabotaje informático: el modus operandi que se utiliza con más frecuencia en el ámbito de sabotaje informático consiste hoy en día sobre todo en la práctica de incendios y atentados con bombas, así como la introducción de los denominados "programas-crash", que borran grandes cantidades de datos en un cortísimo espacio de tiempo.

En el caso de sabotaje que se han descubierto en el ámbito internacional, se han tratado sobre todo de terroristas que actuaban por motivos ideológicos. Estos ven con frecuencia en el ordenador el símbolo del control y de la opresión estatal.

Por esta razón sería conveniente que todas las empresas duplicaran regularmente los datos más importantes y los almacenaran en algún lugar externo al edificio, y que dispusieran de un plan de catástrofes, en especial en relación con los casos de sabotaje.

Hurto de tiempo: se conoce aquellos supuestos tan frecuentes hoy en día en el ámbito del proceso de datos, en los que empleados del proceso de datos, utilizan los ordenadores de la empresa y parcialmente también sus programas, para fines privados y actividades complementarias.

Delitos económicos en general: las posibilidades de manipulación del ordenador son aprovechadas no sólo por empleados que perjudican a la propia empresa, sino también por la gerencia de empresas que trabajan fraudulentamente para perjudicar a la competencia o a organismos estatales. En los casos descubiertos hasta el momento se trataba ante todo de manipulacines de cuentas, balances, lista de inventarios y declaraciones de impuestos elaborados por el ordenador.

CARACTERISTICAS DE LOS DELITOS INFORMATICOS. DESARROLLO FUTURO Y DIFICULTADES DE AVERIGUACION

Permanencia y automatismo del hecho: La característica más evidente que evidencia la criminalidad informática de la criminalidad contra la propiedad en general, está constituida por la especial permanencia en la comisión del hecho.

La posibilidad de repetición que sirve de base a este fenómeno se fundamenta en la rígida organización que normalmente caracteriza la forma del trabajo del proceso de datos, de forma que si el autor encuentra una laguna, en cualquier momento podrá aprovecharse de ella y en este caso a veces se puede advertir la irregularidad a través de un cambio planificado del lugar de trabajo (job-rotation).

Sumas de daños: La permanencia del hecho, a la que acabamos de hacer referencia, constituye una de las causas de los daños tan elevados que producen los delitos informáticos, que es otra de las características de esta forma de criminalidad.

Con ello se confirma la tendencia que cada vez son más elevadas las sumas de daños que son ocasionadas sobre todo porque en el ámbito de la criminalidad informática se trata de dinero contable, cuya cantidad máxima no tiene porqué limitarse, como en cambio sucede en el objeto de las clásicas defraudaciones, que se limitaría a la cantidad de dinero que se encuentre en la caja.

Dificultades de averiguación: Las dificultades de averiguación que caracterizan el ámbito de proceso de datos radican, no en el ordenador, sino en el elevado número de procesos individuales ejecutados. La falta de visualización de los datos almacenados electromagnéticamente también dificulta de forma muy considerable la averiguación de las manipulaciones.

Este problema de averiguación que aquí se plantea (y que ha sido descrito de forma expresiva por la criminología americana como Second-hand) sólo puede resolverse si se reduce mediante un adecuado control informático de los revisores, auditores y funcionarios encargados de la persecución, el tiempo de búsqueda de la información.

Medidas para el descubrimiento de delitos informá-ticos: A fin de reducir al mínimo los riesgos de la criminalidad informática es importante, además, que las medidas preventivas de la empresa no sólo se dirijan a evitar, sino a también a descubrir esta clase de delitos. Como ya hemos dicho, el descubrimiento de delitos informáticos puede revestir considerables dificultades cuando el autor está en situación de manipular los controles y los balances de la empresa. Con frecuencia también en el hurto de software es difícil descubrir qué programas y qué datos se copiaron y utilizaron en el centro de cálculo ajeno. Por ello, si la

instalación de procesos de datos administra direcciones de clientes, puede resultar indicado, por ejemplo, almacenar también las direcciones privadas de los responsables de la seguridad o de los dueños de la empresa, pero de forma errónea (por ejemplo con un nombre falso). Así, si esta persona recibe una oferta de la firma competidora con la misma clase de error en la dirección, por lo menos tendrá conocimiento de que se han copiado los datos de los clientes de la empresa.

A este respecto, el Código Penal Alemán, para los fraudes por medios mecanizados o automatizados, y defraudaciones de fluido eléctrico y otras análogas, dentro del Capítulo "Estafas y otras Defraudaciones" incluye el parágrafo 265 a. que dice: "el que obtiene de forma subrepticia, con la intención de no pagar el precio, la prestación de un aparato automático, o de una red de comunicaciones públicas, el trasporte por un medio público de transporte, o el acceso a una representación u otra institución, será penado con...".

Asimismo, el Código Penal Alemán reprime en su parágrafo 263 a. "quien con la intención de conseguir una ventaja patrimonial ilícita para sí mismo o para otro, cause un perjuicio patrimonial a un tercero, influyendo sobre el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos, o influyendo en la elaboración a través de una intervención ilícita".

EN LO QUE RESPECTA A ESPAÑA

Y conforme conclusiones del Congreso sobre Derecho Informático, organizado por la Facultad de Derecho de Zaragoza durante el año 1989, debemos destacar:

Definición y características del delito informático: delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas.

División de delitos informáticos: pueden dividirse en tres grandes bloques:

a) uso indebido o manipulación fraudulenta de elementos informáticos de cualquier tipo, que posibilitan un beneficio ilícito, tal cual es el fraude informático;

b) casos de vandalismos, terrorismos, etc. cuya finalidad es provocar un perjuicio, con motivo de venganza, extorsión, etc. atentan contra la integridad de los elementos informáticos tal como es acciones físicas;

c) delitos relacionados con la integridad de la propiedad intelectual de los elementos informáticos, especialmente del software, tal como es piratería del software.

Al no existir regulación legal se ha optado por calificar de delictiva toda acción que de forma voluntaria causa un perjuicio a alguien independientemente de que produzca o no un beneficio a su autor. Y de inocua la que no provoca daño a nadie ni beneficia al autor.

Fraudes informáticos: Se puede definir como toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático por medio de la cual alguien trata de obtener un beneficio ilícito.

Elementos: el sujeto, autor o autores de la conducta fraudulenta; el medio, sistema informático sin el cual no se podría llevar a cabo la acción; el objeto, el bien que produce el beneficio ilícito.

Clasificación de los perjuicios: a) perjuicio económico directo: existe una apropiación de bienes, es uno de los pocos que puede ser perseguido y castigado según la legislación tradicional, el problema no es tanto descubrirlo, sino como probarlo; b) perjuicio económico indirecto: no se produce una apropiación de bienes tangibles o valorables, ejemplo: sustracción de información confidencial de carácter económico, comercial, etc. que dañan los intereses de la organización a medio o a largo plazo de forma difícilmente cuantificable; c) perjuicios intangibles, casos poco frecuentes, pueden consistir en la manipulación de programas con la finalidad de deteriorar el prestigio de la empresa para la que se trabaja.

CARACTERISTICAS DE LA ACTIVIDAD INFORMATICA QUE INCIDEN EN LA COMISION DE LOS FRAUDES

Concentración de la información, existe la tendencia a concentrar la información en grandes bases de datos sobre la que interaccionan multitud de usuarios, que acceden a cualquier tipo de información una vez penetradas las medidas de control de accesos.

Ausencias de registros visibles, no existe la posibilidad de descubrir un hecho fraudulento por simple inspección visual al estar la información gravada en forma de impulsos eléctricos.

Los programas y los datos pueden alterarse sin dejar rastros, la alteración del programa o datos grabados en soportes magnéticos puede hacerse sin dejar ni rastro, salvo que se hallan adoptado las medidas de control necesarias.

Fácil eliminación de pruebas, es muy fácil hacer desaparecer programas manipulados o ficheros de datos alterados, pulsando una tecla o emitiendo una instrucción de borrado.

Complejidad del entorno técnico, incluso los sistemas más sencillos presentan una gran complejidad en términos de capacitación técnica.

Dificultad para proteger los ficheros mecanizados, la protección de la información almacenada en soportes magnéticos es muy compleja.

Concentración de funciones, el concepto de segregación de funciones incompatibles suele ser inexistente en los centros de procesos de datos.

Carencia de controles internos en las aplicaciones, que son débiles ante los intentos de manipulación fraudulenta.

Controles ineficaces para el personal técnico, éstos pueden ser soslayados por técnicos informáticos de una cierta calificación.

Dispersión territorial de los puntos de entrada al sistema, para acercar la informática al lugar donde se encuentra el usuario o donde produce los datos de entrada.

Dependencia de redes públicas de transmisión de datos, no es posible establecer medidas de control sobre las redes públicas, sólo sobre los mensajes propios.

TIPOLOGIA DEL FRAUDE INFORMATICO

Sustracción de dinero o documentos que los sustituyan, emisión de cheques auténticos y ficticios por el ordenador, etc.

Sustracción de mercancías, a través de la manipulación de sistemas mecanizados de control de inventarios para hacer desaparecer mercancías, introduciendo movimientos de salida falsos o de no registrar movimientos de entrada.

Sustracción de valores negociables o documentos que sirvan de soporte para el intercambio de mercancías o dinero, casos de apropiación de acciones, valores, participación en fondos de inversión, etc.

Sustracción de servicios, mediante manipulación de los sistemas de medición, registros, facturación y seguimiento de cobros, también la utilización de los dispositivos informáticos en provecho de los empleados de la empresa.

Sustracción de software, lo que se sustrae y generalmente se vende es una copia, los informáticos suelen pensar que las aplicaciones desarrolladas por ellos, son en cierto modo suyas y que la empresa que les ha pagado tiene sólo un relativo derecho de propiedad sobre ellas.

Sustracción de información, en la actualidad es uno de los delitos menos desarrollados, pero que pueden alcanzar una mayor tasa de perjuicios para las empresas afectadas, pudiendo denominarse "espionaje industrial realizado por procedimientos informáticos".

COMO SE REALIZA EL FRAUDE INFORMATICO
(según Donn Parker)

Introducción de datos falsos: es el método más sencillo y más utilizado, consiste en manipular las transacciones de entrada, con el fin de introducir

movimientos falsos, o eliminar las transacciones verdaderas que deberían haberse introducido. Un ejemplo puede ser la introducción desde un terminal inteligente conectado a un ordenador central de transacciones falsas, para producir la emisión de cheques fraudulentos.

El caballo de Troya: el método consiste en introducir dentro de un programa de uso habitual, una rutina o conjunto de instrucciones, por supuesto no autorizadas, para que dicho programa actúe en ciertos casos de forma distinta a como estaba previsto.

Para utilizar este método de fraude es preciso poseer una capacitación técnica suficiente, al menos saber programar y tener acceso al programa para poder manipularlo.

Es éste un método difícil de detectar, pero fácil de prevenir instituyendo unos estrictos procedimientos de catalogación y descatalogación de programas, de forma que sea imposible acceder a ningún programa para su modificación sin los correspondientes permisos, y una vez que éste haya sido modificado, comprobar que el programa funciona correctamente, modificado en lo que se pretendía y que el resto siga igual.

Como ejemplo típico expondremos un caso real sucedido en España. El autor al parecer un ex empleado del centro de proceso de datos de la entidad o de una entidad de crédito, introdujo una rutina dentro del programa del tratamiento de cuentas corrientes, por la que un día determinado, aproximadamente seis meses después de haber cesado el empleado en su trabajo, y a una hora determinada entre las 11,00 y 11,30 se autorizase el pago de un talón de una cuenta concreta sin consultar el saldo, posteriormente la misma rutina borraba parte del programa, con lo que se eliminaba el rastro de la comisión del delito. El fraude fue de unos diez millones de pesetas y no se pudo probar la autoría del mismo.

La técnica de Salami: es la modalidad de fraude más sencilla de realizar y la que menos probabilidades de ser descubierta tiene. El procedimiento consiste en introducir o modificar unas pocas instrucciones en los programas para reducir sistemáticamente en unos céntimos las cuentas corrientes, los saldos de proveedores, etc, transmitiéndolos a una cuenta corriente que se abre con nombre supuesto y que controla el defraudador. Resulta muy difícil descubrir este tipo de fraude, porque no se produce ninguna señal de alarma.

Super zaping: consiste en el uso no autorizado de un programa de utilidad para alterar, borrar, copiar, insertar, o utilizar en cualquier forma no permitida, los datos almacenados en el ordenador o en los soportes magnéticos. El nombre de esta técnica viene de un conocido programa de utilidad "superzap" que es como una llave que abre cualquier rincón del ordenador por protegido que pueda estar, es un programa de acceso universal. Cuando se descubre la alteración de los datos se piensa que ha sido un funcionamiento inadecuado del ordenador o una transacción errónea. En la práctica es imposible probarlo.

Puertas falsas: el método consiste en la producción de interrupciones que hacen los programadores para el chequeo del programa, con lo que se dejan puertas falsas para entrar en él. El problema que plantea este método es tener la certeza de que cuando los programas entran en proceso de producción normal todas las puertas falsas hayan desaparecido. Este método de fraude requiere una especial cualificación técnica por parte de los autores, lo que reduce considerablemente el espectro de personas sobre las que podría sospecharse.

Bombas lógicas: es el procedimiento de sabotaje más comúnmente empleados por los empleados informáticos descontentos que antes de abandonar sus puestos de trabajo dejan una bomba lógica o bomba de tiempo, para producir daños en un momento posterior a su marcha de la empresa. Estas bombas se usan como medio de sabotaje, venganza o placer de perjudicar. El método consiste en introducir en un programa un conjunto de rutinas no utilizadas generalmente ni autorizadas para que en una fecha o circunstancia predeterminada, se ejecuten desencadenando la destrucción de información almacenada en el ordenador, distorsionando el funcionamiento del sistema, provocando paralizaciones intermitentes, etc.

Ataques asincrónicos: este procedimiento es el más complejo desde el punto de vista técnico, no se tiene noticia de la comisión de ningún fraude con él, aunque con su complejidad bien podría ser de los cometidos y no detectados hasta ahora.

La técnica se basa en la forma de funcionar de los sistemas operativos y sus conexiones con los programas de la aplicación a los que sirve y soporta en su ejecución.

El sistema operativo es el conjunto de programas que gobiernan y controlan el funcionamiento del ordenador y de todos sus dispositivos periféricos,

la entrada de los datos que debe ser procesada por los programas, la ejecución de éstos y la salida de información elaborada en los procesos hacia los dispositivos de salida. Otra función fundamental del sistema operativo es optimizar la ocupación de memoria central reasignando áreas en función de las necesidades de cada uno de los programas que están en ejecución en cada momento. También es quien controla y maneja todos los errores que pueden producirse, tanto en el ordenador como en el programa que sea ejecutado, avisando al operador por medio de mensajes de cualquier situación anómala que se produzca.

Los sistemas operativos funcionan en forma asincrónica, estableciendo colas de espera que van desbloqueando en función de la disponibilidad de los datos o recursos que estaban esperando.

Recogida de información residual: se basa en aprovechar los descuidos de los usuarios o técnicos informáticos para obtener información que ha sido abandonada sin ninguna protección como residuo de un trabajo real efectuado con autorización.

Puede hacerse de dos formas distintas: l) Método físico: consiste en recoger el material que se desecha en las papeleras como listado de pruebas de programas, fotocopias de documentos reservados, etc.; 2) Método electrónico: se basa en aprovechar las finalizaciones de ejecuciones de trabajos reales en el ordenador para obtener la información residual que ha quedado en memoria que no se ha tenido la precaución de borrar.

Divulgación no autorizada de datos reservados: se trata de la sustracción de información confidencial o espionaje industrial, realizar la copia de un fichero mecanizado es tan rápido y simple que es una forma de delito prácticamente al alcance de cualquiera.

Pinchado de líneas: es una técnica bastante generalizada para obtener información de forma clandestina. Todo lo que se necesita es un pequeño grabador, un cassette, un módem para demodular las señales telefónicas analógicas y convertirlas en digitales y una pequeña impresora para listar la información que se ha captado.

El procedimiento más eficaz para proteger la información por línea de comunicación, es la criptografía, aunque es un procedimiento poco extendido por

la escasa amenaza que suponen hoy en día los pinchados ilegales y por el costo relativamente caro de los dispositivos criptográficos.

Simulation and modeling: los ordenadores son una herramienta potentísima para efectuar simulación de situaciones, que permiten estudiar las consecuencias previsibles, sobre el comportamiento de una empresa, inversiones, estadísticas, etc.

El ordenador ha servido también para planificar y simular la comisión de un delito antes de realizarlo, aunque en realidad escasean los delitos cometidos por este método.

Otra clasificación realizada por Miguel Ramallo Romero y María Cinta Castillo Jiménez, incluye a:

Los hackers: son esa legión de jóvenes fanáticos de la informática con un ordenador personal, un módem y una gran imaginación que son capaces de acceder a través de una red pública de transmisión de datos al sistema informático de una empresa, institución bancaria, etc., introduciéndose en él. Este fenómeno aún no ha proliferado en España, en otros países esta forma de delincuencia está generalizada.

Las técnicas utilizadas por los hackers se basan en la oportunidad y el esfuerzo, para combatir este tipo de intrusos se establecen los habituales controles de acceso a la información. Uno de los problemas más graves con el que se enfrenta el hackers es hacer frente a las facturas de la compañía telefónica por la utilización masiva de las líneas de comunicaciones. Estos genios, suelen para combatirlo, puntear unas líneas telefónicas para desviar los cargos hacia otros usuarios. Su principal objetivo es penetrar en un sistema informático, para ello: 1) deben encontrar el número de teléfono que les permita conectar con el ordenador, 2) descubrir el identificativo que le permita abrir la cesión de trabajo, 3) averiguar la clave de acceso que le autorice a entrar en las áreas o ficheros reservados.

Se pueden destacar tres tipos de medidas de protección contra los accesos no autorizados a través de líneas de comunicación, dos son lógicos (de software) y un tercero físico (de hardware).

a) la primera consiste en desconectar la comunicación al tercer intento de acceso utilizando una clave errónea, e informar a quien proceda de que ha habido un intento de penetración en el sistema;

b) la segunda es no facilitar por pantalla ninguna información hasta tanto no se halla verificado la identidad de la persona que se ha conectado;

c) por último, un procedimiento bastante eficaz para eliminar el riesgo de ser víctima de los hackers, o de cualquier tipo de acceso indebido, vía línea de comunicaciones, consiste en tener un sistema de "call back" o de devolución de llamadas.

La eficacia de este dispositivo se basa en que cuando un usuario conecta con el sistema y se identifica válidamente, queda registrada su identificación y a continuación antes de comenzar la cesión de trabajo, el sistema investiga y desencadena una llamada del ordenador central al número real del usuario identificado.

La piratería del software: según la Organización Mundial de la Propiedad Intelectual, se entiende por software, al programa, conjunto de instrucciones que cuando se hallan en un soporte y formato legible por el ordenador dotan a este de la capacidad de procesar información en orden a realizar una determinada función o tarea, o calcular un determinado resultado.

El material de soporte es cualquier otra documentación, aparte del programa y de su descripción, creado para servir de ayuda a la comprensión y utilización de los programas, por ejemplo el manual del usuario.

Los elementos que se incluyen en la definición son bastantes heterogéneos, incluyen elementos tangibles, como puede ser el disco donde está grabado el programa, que es un elemento tangible y el programa grabado en el que es un elemento intangible, por lo que al comprar un disco conteniendo una serie de programas, no sólo no somos propietarios de dichos programas, sino que legalmente ni siquiera tenemos derecho a copiarlos, lo que hemos adquirido ha sido una serie de derechos de uso sobre los elementos intangibles, contenidos en el producto tangible que les sirve de soporte.

CAUSAS QUE DAN ORIGEN A LA PIRATERIA DEL SOFTWARE

Las personas que desarrollan un determinado software son asalariados de una empresa que creen tener sobre el software creado una serie de derechos, sin considerar el salario recibido por ellos.

El segundo factor que interviene, es el hecho que al hacer una copia no se deteriora el original, lo que da la apariencia de ser una acción inofensiva, pero en realidad las empresas dedicadas a la creación de software se ven gravemente perjudicadas y por el contrario las que consiguen las copias de los programas se ven beneficiadas al encontrarse con un programa que no han tenido que encargar ni comprar.

El tercer factor que interviene en el gran desarrollo que tiene la piratería del software, es el precio desproporcionadamente alto que se ha aplicado, a gran parte de los programas que se comercializan.

Actualmente el Código Penal Español en su art. 255 expresa: "será castigado con la pena de... el que cometiere defraudación, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos por alguno de los medios siguientes:

1) valiéndose de mecanismos instalados para realizar la defraudación;

2) alterando maliciosamente las indicaciones o aparatos contadores;

3) empleando cualesquiera otros medios clandestinos".

El art. 248 de este Código expresa en su inciso primero: "cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir un error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno" y en su inciso segundo: "también se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de terceros".

LA VANGUARDIA NORTEAMERICANA

Es de destacar la infraestructura desarrollada en los Estados Unidos para permitir el funcionamiento de la firma digital, utilizada en la actualidad para otorgar seguridad a las transacciones comerciales electrónicas y a la transferencia electrónica de datos.

El comercio electrónico en general, de Internet, en especial, fue ideado para el intercambio de información. Sin embargo, en la actualidad se los utiliza en gran medida para transacciones que requieren el posterior transporte de la mercadería objeto de las transacciones. La compra electrónica será la comercializadora inevitable de la Internet, pero los que la defienden fervorosamente deberían tener en cuenta que los hábitos de los consumidores, son difíciles de romper, ya que generalmente les gusta elegir y tocar las mercancías.

Otro requisito para el asentamiento del comercio electrónico radica en sistemas de pagos eficientes y seguros, pudiendo clasificar estos sistemas distinguiendo entre tarjetas de crédito, cheques digitales y dinero electrónico.

Con respecto a los cheques digitales, este sistema funciona como si se tratare de cheques reales, salvo que el usuario utiliza una firma digital para firmar el cheque y luego transmitirlo en línea (no linee) encuitado.

El usuario necesita una chequera electrónica que actualmente consiste en una tarjeta de tamaño de una tarjeta de crédito que puede contener datos y se inserta en un solté en la mayoría de las computadoras portátiles que se vende en la actualidad. En el futuro la chequera se llevará en una tarjeta inteligente (smart card), que cuenta con un chip y distintos tipos de memoria, que le permitirá generar cheques, llevar su registro de cheques y guardar claves públicas y privadas.

En lo que respecta a la seguridad, en principio, se da por sentado que el medio utilizado es inseguro. Preocupa sobre manera de que puedan ser interceptados datos que circulan por la red de redes Internet, que básicamente constituye el medio de transmisión de datos por excelencia. A esto podemos agregarle otro ingrediente que complica severamente la situación en el sistema norteamericano: La ausencia de terceras partes confiables.

Hasta el momento, lo más efectivo para proteger la información que se transmite, ha sido recurrir al milenario sistema de cifrar la información que se envía.

Esto nos introduce en la ciencia de la Criptografía, que estudia la ocultación, disimulación o cifrado de la información.

La Criptografía tradicional se basa en el concepto de que tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave secreta. Este método se conoce como Criptografía con clave secreta, el que ha tenido dificultades para brindar la seguridad necesaria en este aspecto.

Existe un acuerdo generalizado acerca de que el sistema que mayor seguridad brinda en la actualidad a las transacciones electrónicas e intercambio electrónico de datos es el de la Criptología de clave pública, basada en algoritmos asimétricos, inventada en 1976 en la Universidad de Standford Estados Unidos. En este sistema cada persona obtiene un par de claves, llamadas clave pública y clave privada. Cada usuario debe generar su propio par de claves, por intermedio de un Software confiable.

Por este medio se obtienen transacciones seguras y auténticas con la certeza de la integridad de los datos y la imposibilidad de repudio por parte del emisor. El sistema requiere una infraestructura grande y compleja, pero esencial: Sin ella los usuarios no podrán saber con quién están tratando en la red, a quién le están enviando dinero, quien firmó un documento o si la información fue interceptada y alterada mediante la transmisión. Por ello los usuarios demandarán una fuerte infraestructura de administración con manejo de claves basadas en autoridades certificantes que operen bajo estrictas normas predeterminadas.

Se han advertido entonces distintas posturas legislativas respecto de la validez del documento electrónico: a) Una postura amplia en que el legislador establece la validez del documento electrónico, sin hacer referencia a su soporte material ni al tipo de lenguaje a utilizar. Tampoco se analiza o se ajustan otras normas que hacen referencia al documento tradicional (proyecto del Estado de California y Florida);

b) Una postura restringida en que el legislador se preocupa no sólo de establecer la validez jurídica del documento electrónico, sino también de

reglamentar su uso, a la vez que determina detalladamente la infraestructura técnica y operacional que se utilizará para la inserción del mismo en la práctica comercial (Utah y Georgia);

c) Una postura detallista en que el legislador revisa todo el cuerpo legal para derogar, modificar o agregar normas que hagan compatibles el sistema con el documento electrónico (proyecto del gobierno de Alemania); y por último,

d) Algunas combinaciones, donde se encuentra un sistema de intervención junto con algunas características de las posturas antes referidas (proyecto de ley de Italia y Chile).

Existen en los Estados Unidos restricciones impuestas por el gobierno al desarrollo y difusión de las tecnologías criptográficas. La National Security Agency (N.S.A.) fue creada por orden del presidente Truman en 1952, siendo su función primordial la intervención en el área de comunicaciones, interceptando y descifrando las comunicaciones secretas de otros gobiernos.

Se sostiene en los Estados Unidos que el Gobierno y la Industria deben trabajar conjuntamente a los efectos de crear una infraestructura que brinde seguridad y permita el desarrollo de productos que incorporen elementos de criptografía, sin menoscabar la seguridad Nacional y Pública.

La industria participará en la definición de algoritmos y protocolos standar, y desarrollará productos de claves de encriptado adecuados para la protección de los sectores públicos y privados. El Gobierno colaborará estableciendo estándares para la infraestructura de administración de claves y proveerá un mercado para productos de seguridad.

Resulta claro para las comunidades legales y técnicas de los Estados Unidos que el comercio electrónico requerirá mayor autenticación y certificación de los documentos electrónicos para asegurar la aceptación de los actos. Esto es particularmente cierto para aplicaciones comerciales en el ámbito internacional, donde de las diferencias en el derecho y la práctica, y las dificultades en establecer relaciones entre partes, aumentan la necesidad de mecanismos que brinden seguridad a las transacciones. El futuro del comercio electrónico internacional descansa en la importancia que los contratantes otorguen a la seguridad de la transmisión y contenido de la comunicación, y en la creencia de que esas

comunicaciones tendrán garantizado un adecuado reconocimiento que asegure su aceptación en cualquier jurisdicción, ya sea local o extranjera.

El proyecto Cybernotario propone rectificar la ausencia de seguridad en las transacciones originadas en los Estados Unidos, así como las que se realicen electrónicamente a través de la creación de una oficina "cuasi pública" conocida como cybernotario, cuyo rol será el de combinar experiencia legal y técnica en una sola especialización, y cuyos miembros ejercerán dos funciones distintas pero complementarias.

La primera de esas funciones permitirá que los actos pasados por ante el cybernotario tengan pleno reconocimiento y efectos fuera de los Estados Unidos. La segunda y más importante función surgirá de su capacidad de certificación y autenticación electrónicas de todos los elementos de una transacción comercial electrónica, indispensables para su aceptación por el derecho de los Estados Unidos y de los demás países. Mediante la utilización de la firma digital, el cybernotario, podrá certificar la identidad del emisor de un mensaje, lo que implica la imposibilidad de repudiar el mensaje, dan un alto nivel de seguridad en cuanto al contenido del mismo, fechar la notarización (fecha y hora de su intervención), y su protocolización con fines de archivo.

COLOFON

A lo largo de todo este trabajo hemos hecho referencia a la falta de tipificación específica, en nuestro país, de ciertas conductas ilícitas, sumamente perjudiciales para el patrimonio en su totalidad.

Hemos deslizado también la opinión del profesor Tiedemann, para quien, uno de los motivos por los cuales no existen normas específicas que sancionen este tipo de delitos, se debe a los intereses de poderosos grupos que influyen sobre los órganos legislativos, opinión con la que respetuosamente no coincidimos por estimar que los baches normativos a que éste refiere no se deben a las mencionadas presiones, sino, a la falta de capacitación en el tema informático que trae aparejado la desregulación de conductas cometidas por medio de maquinarias informatizadas, cuya evolución -en la mayoría de los casos- supera nuestro marco normativo legal vigente.

Asimismo se suma a ello la falta de especialización en el tema en análisis de quienes deben dar respuestas a la necesidad de tutelar los bienes jurídicos que

se afectan por esta nueva forma de delinquir, no obstante tener como modelo países, que si bien no ofrecen las mayores garantías, han establecido un notorio mejoramiento en este sentido implementando normas típicas que describen con claridad y suficiencia las figuras delictivas originadas por la informatización en la mayoría de sus relaciones internas e internacionales.

También abona esta deuda legislativa los diferentes problemas económicos y sociales por el que atraviesa nuestro país. En el primero de los casos el elevado costo que insume la instalación de diversas maquinarias, instituciones y especialistas hace que deba tomarse una decisión política de riesgo para las autoridades de turno. En virtud del segundo planteo efectuado en este párrafo, o sea el social, el incremento monetario que significaría un adelanto en la materia recrudecería la crisis social, pues se deberían distraer al menos por un largo período, las necesidades básicas de nuestra sociedad.

Por ello creemos firmemente que, aún cuando la aparición de delitos informáticos circula a una velocidad mayor que la de los legisladores en el campo preventivo y punitivo, es menester, al menos en nuestro país, comenzar creando tipos penales que describan conductas que ya son harto conocidas, como lo vienen haciendo países como Alemania, España y Estados Unidos, tal cual se refleja en los artículos incluidos en sus Códigos Penales, cuya transcripción hemos realizado en el presente trabajo.

Creemos en el dinamismo del derecho, por ello vemos una despreocupación acentuada en nuestros legisladores, que conforme lo investigado, toleran la petrificación de normas que ni siquiera integran nuestro digesto penal, sino que se encuentran contenidas por ejemplo en la ley de propiedad intelectual.

Asimismo y ante el letargo legislativo, nuestra jurisprudencia mayoritaria ha tenido que echar mano a la analogía, que si bien es permitida "in bonam parte", no la creemos conveniente; como también vemos desfavorable que nuestros doctrinarios se debatan en argumentos defensivos y estériles al tratar de encuadrar conductas atípicas realizadas a través de maquinarias informatizadas, únicamente dentro de dos tipos penales como lo son el Hurto y la Estafa.

Además de la analogía a la que hicimos referencia precedentemente, a la cual creemos que no será necesario acudir de existir normas que contengan específicamente las conductas disvaliosas en torno a este tema. No deberemos

caer tampoco, como lo ha hecho la ley de propiedad intelectual, en las llamadas leyes penales en blanco.

No debemos olvidar, al crear estas normas, el principio de legalidad acuñado en nuestra Carta Magna, que nos exige la investigación profunda, amplia y total de todos y cada uno de los hechos de carácter delictivo que lleguen a conocimiento de las Instituciones con jurisdicción para juzgarlos, siendo necesario para ello la creación de estas normas específicas para no desvirtuar este principio Constitucional, como creemos que, actualmente y en la mayoría de los casos, dejamos de lado.

Vemos con gran asombro que la mayoría de la doctrina y jurisprudencia se ha inclinado en encuadrar este tipo de acciones bajo el Art. 162 del Código Penal, el que establece una pena máxima de dos años de prisión, y teniendo en cuenta lo gravoso y perjudicial del detrimento patrimonial, que resulta de la comisión de la mayoría de los delitos que se cometen a través de la informática, nos parece demasiado benévola la pena que establece la referida norma, por lo que, con más razón es imperiosa la necesidad de la creación de las figuras penales que venimos pregonando.

Admitimos necesaria la creación de un capítulo específico dentro del digesto penal vigente donde debería asentarse un articulado referido con exclusividad a los delitos sobre los que nos venimos refiriendo.

Que ello así planteado no hace mas que echar por tierra nuestro convencimiento al comenzar este trabajo, por cuanto la introducción de la informática en los distintos niveles de nuestra sociedad no puede, al menos en forma inmediata, traer aparejada la seguridad que creemos perdida o deficiente, tal cual fuera planteado en nuestra idea original.

Por consiguiente luego de analizar la diversa bibliografía consultada, advertimos que países de mayor desarrollo tecnológico nos han demostrado que con intencionalidad, buen criterio y decisión política han logrado recuperar parte de esa seguridad que pretendemos. También vemos con optimismo que si en nuestro país logramos salir del letargo legislativo en que nos encontramos, creando normas autónomas que describan claramente el accionar de quienes por

medio de su capacitación personal o no, vulneran los mecanismos de control, que en algunos sectores, al menos, se han implementado como desarrollo tecnológico, podremos restablecer parte de la seguridad perdida.

BIBLIOGRAFIA

- "Congreso sobre Derecho Informático" - Año 1989 - Facultad de Derecho de Zaragoza - María Cinta Castillo Jiménez y Miguel Ramallo Romero.

- "Ley de Propiedad Intelectual" nº 11.723.

- "Programa Regional de Cooperación en Informática y Microelectrónica" - Año 1991 - Mario Barreto Gugelmeier.

- "Revista La Ley" - Año 1997 - nº 120 - "La estafa mediante medios mecanizados" - Sandro F. Abraldes.

- "Revista La Ley" - Año 1997 - nº 76 - "Banca, Comercio, Moneda Electrónica y la firma digital" - Horacio M. Lynch.

- "Delincuencia Informática: El software como objeto de conductas disvaliosas" - por Carlos Alberto Cruz.

- "Delincuencia Informática" - Santiago Mir Puig.

- "Revista del Derecho Industrial" - Año 1995 - Nº 21 - Editorial Depalma.