

DELITOS INFORMÁTICOS Y LAS TIC

AUTORA: Alicia Silva Silva *

Institución: Universidad de Carabobo (UC)

Silva_ali@yahoo.com

Silvalicia@gmail.com

RESUMEN

El presente ensayo tiene por objeto analizar la tecnología informática y su influencia en áreas determinantes en la vida social, donde ha surgido una serie de comportamientos ilícitos denominados de manera genérica, Delito Informático. En este contexto, nadie escapa de la enorme influencia que ha alcanzado la informática en la vida diaria: la comunicación, los procesos industriales, las investigaciones, entre otros, son aspectos que dependen cada día más de un adecuado impulso de la tecnología informática. En el resto de este apartado, se examinará brevemente un tipo de delito informático: *la piratería del software*, donde no siempre se cumple la norma con vigor.

Palabras Clave: Delito, Informática, Piratería

Reflexiones Discursivas

En este nuevo esquema, no es posible contar con una definición de delitos informáticos, pues cada país de acuerdo a sus realidades ha formulado un concepto en el cual de ordinario se procura incluir nuevas modalidades delictivas o describir en términos más actuales comportamientos tradicionales que, en razón del medio de comisión empleado adquieren la condición de informáticos.

* Profesora e Investigadora de la Facultad de Ciencias de la Salud de la Universidad de Carabobo. Maestrante en Investigación Educativa, Doctorante en Ciencias Sociales. Investigadora acreditada por la Fundación Venezolana de Promoción al Investigador (FVPI).

Estos cambios experimentados obligan a revisar la opinión de estudiosos e investigadores del Derecho Penal, debido a que la definición de delito informático es compleja, han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta.

Ante este escenario, Palassi (1999), define los delitos informáticos como todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio.

Sobre este aspecto, Casabona (1996:258), se refiere a la definición propuesta por el Departamento de Justicia Norteamericana, según la cual Delito Informático es cualquier acto ilegal en relación con el cual el conocimiento de la tecnología informática es esencial para su comisión, investigación y persecución.

Una clave opinión es la de Davara (1997:155), quien señala que el Delito informático es la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software”.

En concordancia con lo expuesto, se conoce en un plano sustancial tal y como lo señala el ilustre jurista venezolano Arteaga (1995:125), “como un hecho que, en sí mismo o por su forma, lesiona intereses fundamentales de la sociedad, intereses que se consideran básicos para la existencia, conservación y desarrollo del conglomerado social”.

Dada la importancia de esta acepción, Davara (1997) hace una clasificación que responde no sólo a un criterio sistematizador vinculado a las de carácter automático de datos, sino al mismo tiempo a una separación de diversos tipos criminológicos de conducta. Las conductas más significativas desde esta perspectiva podrían agruparse en estas cinco modalidades principales: a) manipulaciones de datos y/o programas, o “fraude informático”, b) copia ilegal de programas (piratería del software), c) obtención y utilización ilícita de datos, o “espionaje informático”, d) destrucción o inutilización de datos y/o programas, o “daños o sabotaje informático” y e) agresiones en el hardware o soporte material informático, principalmente “hurto de tiempo del ordenador”.

Por último, siguiendo a Davara incluye “la informática como instrumento en la comisión de un delito”, distingue dentro de la manipulación mediante la informática dos vertientes diferentes: a) Acceso y manipulación de datos y b) Manipulación de los programas.

Atendiendo a ello, considera que determinadas acciones que se podrían encuadrar dentro de lo que hemos llamado el delito informático, y que para su estudio, las clasifica, de acuerdo con el fin que persiguen, en seis apartados: 1.) Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos, 2.) Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello, 3.) Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas, 4.) Utilización del ordenador y/o los programas de otras persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro, 5.) Utilización del ordenador con fines fraudulentos y 6) Agresión a la “privacidad” mediante la utilización y procesamiento de datos personales con fin distinto al autorizado.

En la actualidad la informatización se ha implantado en casi todos los países. Tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Pese a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos.

A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

Cambios de Paradigmas y Nuevos Comportamientos

Con el transcurrir del tiempo las Tecnologías de la información (TIC) se han convertido en uno de los medios más importantes, así como complemento cultural para el hombre.

Al decir de Boar (1994:15) define las Tecnología de Información y Comunicación (TIC) como la preparación, recolección, transporte, consulta, almacenamiento, acceso, presentación y transformación de la información en todas sus formas (voz, gráficos, vídeo texto e imágenes). Dicha información puede transferirse entre humanos y máquinas y/o máquinas. La gerencia de tecnología de información y comunicación, asegura la apropiada selección, instalación, administración, operación y mantenimiento de los activos de tecnología de información, de forma consistente con los objetivos organizacionales.

Es evidente que el uso de la tecnología de la información y comunicación convierte al individuo en un ente de cambio que enfrenta un mundo nuevo de transformaciones. El poder de la información está disponible para cada ser humano que la consulta en la red y

todo aquel que tenga acceso a Internet tiene seguro el contacto con la información para enfrentar los nuevos retos de la sociedad actual.

De acuerdo con Rojas (1999), las TIC acaparan el poder mundial por sus múltiples beneficios: acorta las distancias territoriales y lingüísticas-culturales, no existe problema con los horarios, e incluso reduce los espacios físicos permitiendo acceso a un libre flujo de información.

Los millones de ordenadores conectados a Internet ofreciendo todo tipo de informaciones y actividades, forman una enorme masa potencialmente valiosa para la educación, pero muy decepcionante si no se accede con una buena herramienta y con buena metodología. No hay que olvidar que la mera incorporación de datos no constituye información. Sólo cuando existe un análisis de los datos y una estructura que permita acceder rápida y efectivamente a los mismos, podemos hablar de información.

El desarrollo de la tecnología ha dado lugar a la aparición de nuevos comportamientos que no encuadran dentro de las descripciones típicas convencionales. En efecto, el legislador entre otros bienes jurídicos, la propiedad, la privacidad de las comunicaciones, la propiedad intelectual, la autenticidad de los documentos, entre otros.

No obstante, no consideró que tales hechos podrían ser perpetrados a través de medios informáticos, electrónicos o telemáticos, de allí que, al margen de las tesis que, aplicando una interpretación progresiva de la ley penal, pudieren inclinarse por la inclusión de esas conductas dentro de tipos penales tradicionales, cada vez más se observa que, ante las limitaciones impuestas por el principio de legalidad penal que proscribe la analogía y la

interpretación extensiva, actualmente los legisladores de los diferentes Estados introducen modificaciones en sus Códigos Penales o, por tratarse de una materia tan dinámica y en constante evolución, propician la creación de leyes especiales, sustancialmente de naturaleza penal.

Hoy puede advertirse al hacer un examen de derecho comparado, la tendencia a regular una amplia gama de conductas en las que los sistemas que utilizan tecnologías de información son objeto de comisión de delitos o se utilizan como medio de comisión de delitos de diversa naturaleza: patrimoniales, atentatorios contra la intimidad de las personas, la autoría intelectual, la propiedad industrial o la información, entre otros bienes jurídicos o, inclusive, cuando a través del uso de esa tecnología, se afectan los propios sistemas a fin de causar daño a una persona o su propiedad, como es el caso de la transmisión de virus informáticos.

Sin embargo, tales legislaciones tienen como denominador común el haber abordado el problema sólo desde la óptica del bien jurídico que en un momento determinado ha resultado mayormente vulnerado, de allí que no se aprecie una regulación sistemática que proponga soluciones o por lo menos controles globales al problema.

Algunos han sostenido que en tipos penales tradicionales contemplados en las actuales legislaciones podrían subsumirse algunos comportamientos perpetrados en perjuicio o a través del uso de medios informáticos; tal es el caso de los delitos de estafa, hurto y algunas modalidades atentatorias contra el derecho de autor.

A ello se opone que en esos delitos el legislador ha dirigido su acción a tutelar el patrimonio económico, por tanto, el hecho de que la información almacenada en la memoria de un computador, o en general, incorporada a un sistema que utiliza tecnologías de información no sea materialmente susceptible de apropiación, conlleva a la imposibilidad de aplicación de tales dispositivos legales. Ni siquiera mediante la interpretación progresiva de la ley podría lograrse este cometido, pues se vería seriamente afectado al principio de la legalidad.

Es precisamente, que la conducta desplegada a través del acceso a un sistema que utilice tecnologías de información no podría encuadrar en un tipo penal tradicional, como el hurto cuando por ejemplo, un sujeto conoce u obtiene la contraseña para penetrar en el sistema con el fin de que se verifique la transferencia de una cuenta bancaria ajena a otra creada por él. Dicha conducta difícilmente podría encuadrar en el apoderamiento de que trata el Código Penal máxime si la acción recayó sobre la información, independientemente de que los efectos y los fines de carácter económico.

Piratería del Software

La piratería de software es atentar contra los derechos de la propiedad intelectual. Se produce la piratería cuando: 1) un individuo o entidad ofrece copias ilegales, CD-ROM, aplicaciones descargables o números de serie gratis, a cambio de dinero o mediante trueque 2) un individuo proporciona un producto educativo sin autorización o a particulares o empresas no autorizados, 3) un individuo instala o utiliza el software sin una licencia debidamente autorizada, o cuando lo hace en más sistemas de los que está autorizado.

Existen varias formas de piratería, entre las más resultantes se conocen:

- **La piratería del usuario final:** la forma más común de la piratería, el usuario final o la organización copian el software en más equipos de los que el acuerdo de la licencia permite (por defecto cada máquina que utiliza el software debe tener su propia licencia).
- **Piratería de carga de disco duro:** los distribuidores de equipos informáticos sin escrúpulos cargan previamente software sin licencia en los equipos, y no suministran a sus clientes las licencias necesarias.
- **Piratería de falsificación y de CD-ROM:** los vendedores ilegales, que con frecuencia se organizan en redes delictivas, transmiten software falso como si fuera auténtico, intentando emular el embalaje del producto con el nombre de la empresa y las marcas comerciales propietarias.
- **Piratería por Internet:** se trata de cualquier tipo de piratería que implique la distribución electrónica no autorizada o la descarga desde Internet de programas de software con copyright.

El punto de inflexión de los cambios ocurridos, arrojan que sólo en el año 2000 el Business Software Alliance (BSA), adoptó medidas contra la piratería en todo el mundo en más de 25.000 casos, y en más de 120.000 ocasiones, se contactó con BSA para comunicar algún caso de piratería de software, o para consultar sobre la conformidad de licencias. Las

consultas e informes enviados a BSA se recibieron a través de sus miembros y, principalmente, de las 65 líneas directas en todo el mundo.

Este replanteamiento sería factible al menos en el ámbito del software de sistema si se aplica la teoría de que hardware y software son inseparables. Una vez aplicada, se puede concluir entonces; que las licencias de software no se deberían otorgar a las empresas que ensamblan PCs (HP, IBM, Dell, entre otros, sino a los desarrolladores de CPUs (Intel, AMD, etc). De tal manera que por cada CPU vendido (hardware); se incluya también el sistema operativo (software).

Asimismo, cualquier consumidor que comprase equipo de cómputo (fuese de marca o no), o un CPU para una actualización del hardware, tendría la certeza de que hardware y software están completamente integrados (el CPU trabajaría de manera adecuada con el software, al menos en teoría), además de que el empleo de este esquema proporcionaría al usuario la convicción de que su software de sistema esta legalizado.

Con la salvedad de que para hacerlo verdaderamente atractivo para el consumidor, este software debería contar aparte de las utilerías necesarias, versiones básicas de un procesador de textos, hoja de cálculo, manejador de base de datos y navegador.

En el estudio realizado por la BSA e IPSOS revela que 55% de los estudiantes encuestados reconocen haber experimentado problemas relacionados con virus y spyware por actividades de descarga ilegal y sólo el 30 % es conciente de esta situación.

Según el último estudio realizado por BSA e IPSOS, compañía internacional de investigación (www.ipsos.com), más de la mitad de la población estudiantil de colegios y universidades que ha descargado programas sin licencia o ha intercambiado archivos con derechos reservados, se ha visto enfrentada a virus informático y spyware (software que

recopila información de un computador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del mismo).

En el análisis de los datos de la BSA en Venezuela, es importante destacar que la tasa de piratería en fue del 79% por ciento en el 2004, 7% más que en el 2003 y las pérdidas por piratería de software ascendieron a US\$ 71 millones de dólares, según el estudio de piratería mundial de software publicado realizado por IDC, el líder global en investigación de temas de tecnología.

Las pérdidas por piratería de software ocasionan un gran impacto económico en los países. Cada copia de software utilizada sin la licencia apropiada cuesta ingresos fiscales, empleos y oportunidades de crecimiento para mercados de software que están en desarrollo. En el caso venezolano, estamos hablando de US\$ 71 millones de dólares perdidos por la industria del software y aproximadamente US\$ 11.4 millones de dólares que el Estado Venezolano perdió en contribuciones fiscales.

En Venezuela el valor del software pirateado aumentó como resultado de un crecimiento superior a seis por ciento en la industria mundial del software para PC y la caída del dólar estadounidense, que fue superior a seis por ciento con respecto a las otras monedas del mundo.

La piratería en Venezuela sube o baja como consecuencia de una compleja ecuación que incluye por un lado la educación y el cumplimiento de las leyes ya existentes y, por otro, el ingreso de nuevos usuarios al mercado, la simplificación del acceso a software pirateado y/o nuevos factores externos, como la certeza de contar con el proveedor adecuado. No obstante, el incremento de 7% en los índices de piratería, el trabajo que

vienen realizando las autoridades nacionales va por un buen camino pero debería reforzarse y ser más contundente.

Los programas educativos de BSA, el fomento de políticas públicas y los esfuerzos de aplicación y ejecución de la ley en Venezuela continúan teniendo un impacto positivo sobre el problema de la piratería. Pero la afluencia continua de nuevos usuarios en mercados emergentes y la creciente disponibilidad de software pirateado, principalmente a través de la Internet y redes P2P, demuestra que la educación permanente es esencial.

A futuro y por las razones señaladas en el espacio anterior, la BSA continuará su esfuerzo de contener el crecimiento de la piratería, estimulando así las economías locales, creando empleos, generando ingresos fiscales y promoviendo la inversión en la innovación tecnológica para el futuro.

A modo de Conclusión

En el artículo se reafirma como señala Cuervo (2000), “que el delito informático se caracteriza por las dificultades que entraña descubrirlo, probarlo y perseguirlo”. En el caso particular de la piratería del software, son delitos, que en la mayoría de los casos no se denuncian, para evitar la alarma social o el desprestigio por un fallo en la seguridad. Es absolutamente central en la organización de nuestras sociedades modernas y que se transforma en la medida en que se transforman también las sociedades.

En esta evolución del contexto en que se desarrolla el trabajo cotidiano con el uso de la informática, es fundamental el pasaje de una sociedad inclusiva, que en términos de Michael Foucault ha sido descrita como el pasaje de una “sociedad disciplinaria” a una

“sociedad de control”. Y en esto juega un papel esencial la difusión de la informática y, junto a ella, una ruptura en la concepción del tiempo y el espacio.

De las derivadas consecuencias de las nuevas realidades de la tecnología y la informática, que se han venido desarrollando en este mundo globalizado debido a su acelerado desarrollo y su incidencia directa en varios ámbitos de la sociedad han alcanzado el rango de bienes jurídicos protegidos por el ordenamiento jurídico, particularmente por el Derecho Penal.

Bajo una mirada que privilegia deliberadamente, se puede considerar que el nuevo Código Penal Venezolano es una herramienta de gran valor para jueces, juristas y abogados que permitirá el tener que efectuar construcciones jurídicas artificiosas para penar conductas socialmente reprochables que necesitaban tener su cabida en el Código Penal del siglo XXI.

REFERENCIAS BIBLIOGRÁFICAS

- ARTEAGA, Alberto (1995). *Derecho Penal Venezolano*, 7ª Edición,. Paredes Editores. Caracas.
- Constitución de la República Bolivariana de Venezuela, Gaceta Oficial No. 5435. Caracas.
- CUERVO, José (1999). *Delitos informáticos: protección penal de la intimidad*. Revista de Derecho Informático. Alfa Redi. España.
- DAVARA, Miguel. (1997) *Manual de Derecho Informático*, Editorial Aranzadi, Pamplona. Colombia.
- DAVARA, Miguel (1996). *De las Autopistas de la Información a la Sociedad Virtual.*, Editorial Aranzadi. México.

- Ley Especial contra Delitos los Delitos Informáticos. Gaceta Oficial. Nro.37.313, martes 30 de octubre de 2001.
- Ley Orgánica de Ciencia, Tecnología e Innovación, Gaceta Oficial No.37.291, miércoles 26 de septiembre de 2001.
- PALAZZI, Pablo A. (2000). *Delitos Informáticos*, AD-HOC, Buenos Aires.
- ROMEO, Carlos (1995). *Los llamados delitos informáticos*, Revista de Informática y Derecho, UNED, Centro Regional de Extremadura, Mérida, España.
- ROJAS, Luis (1999). *En Dirección a la Postcomunicación*. Revista Telos 1 (1) 11-25, URBE. Venezuela.