# Algunos problemas puntuales. Experiencias Legislativas y Jurisprudenciales en Latinoamérica

YARINA AMOROSO FERNÁNDEZ

*Especialista del Ministerio de Justicia de Cuba.*
*Presidenta de la Sociedad Cubana de Derecho e Informática.*

## INTRODUCCIÓN:

Estamos frente a un tema original: el binomio "Nuevas Tecnologías y Derecho", los que en interacción generan nuevos fenómenos y su vez demandan respuestas a corto, mediano y largo plazo. También para encauzar la acción ante este binomio se requiere un esfuerzo sostenido, capacidad informática y jurídica específicas, así como determinante voluntad política de romper los moldes tradicionales y caducos. De esta forma podremos enfrentar, por un lado un lado las nuevas tecnologías que son un medio y no un fin; y por otro, el desafío que las mismas han provocado en nuestro entorno social y cultural.

La expresión más comunmente utilizada en nuestro medio para expresar estas nuevas tecnologías: La Informática, incide en todas las ramas del Derecho.

La Informática como objeto de Derecho, demanda de éste respuestas tendentes a establecer nuevas reglas jurídicas en materias tales como: la promoción y protección del software y la industria Informática; el valor probatorio del documento electrónico; las materias contractuales en la adquisición de bienes y servicios informáticos.

La égida Derecho al reclamo de la Informática alcanza además a todo lo relativo al flujo de datos Trasfronteras y la defensa de los derechos individuales, frente a los riesgos que la información acarrea para las libertades públicas y privadas.

También el Derecho se ha tenido que pronunciar en cuanto a las particularidades de los contratos laborales en el contexto de servicios y producciones informáticas y las enfermedades profesionales derivadas del uso de las nuevas tecnologías y más recientemente las regulaciones que rigen el régimen jurídico del Teletrabajo.

Otro tema emergente de las nuevas tecnologías y que ha reclamado protección del Derecho es el referido a los bancos de datos así como los contratos de transferencia de tecnologías informáticas, entre otros múltiples aspectos.

Pero como es de presumir, el desarrollo de la rama jurídica asociada a la informática está en relación estrecha con el grado de difusión de esta última y más aún con el tipo de política informática aplicada, por eso a continuación intentaré aproximarme a experiencias latinoamericanas[1] y especialmente la experiencia cubana, para ello haré referencia algunas soluciones legislativas, jurisprudenciales y la doctrina de los temas que abordaré en este curso de Maestría, aunque el tema central de estas experiencias están referidas fundamentalmente al Derecho Penal de la Informática, y más aún si se puede hablar una "filosofía del Derecho Penal de la Informática"

A continuación les voy a exponer en tópicos independientes y muy sucintamente tratado a mi juicio las principales realizaciones en materia de Derecho de la Informática en Latinoamérica. Así como aquellas que se refieren al otro segmento de interés de estudio en el devenir de la incidencia Derecho e Informática, este caso en el que el Derecho es el objeto de estudio y la informática la herramienta, lo que metodológicamente se ha identificado como Informática Jurídica.

## I. MUY BREVE REFERENCIA DEL DERECHO DE LA INFORMÁTICA EN LATINOAMÉRICA. EXPERIENCIAS EN CUBA.

a)- ¿Qué entiendo por Derecho de la Informática?:

[1] Carlos Ferreyros, "Aspectos metodológicos del delito informático", Notas del curso Nuevas Tecnologías y Derecho, UNED, mayo de 1995. Mérida, España.

Como parte también consustancial al proceso de "Informatización de la Sociedad", es necesario contar con el orden legal que nos permita proteger a la sociedad ante las arbitrariedades y abusos que puedan cometerse en el uso indebido de las nuevas tecnologías de la información y la comunicación: así como ordenar los procesos de desarrollo de aplicaciones de estas tecnologías, para que cuenten con las garantías técnicas y jurídicas que permitan su generalización y comercialización como bienes y servicios de valor patrimonial, tutelares por el Derecho a pesar de tener en muchas ocasiones una naturaleza inmaterial.

El impacto social de las nuevas tecnologías incide en casi todas las ramas tradicionales del Derecho tales como: Constitucional, Civil, Laboral, Administrativo, Mercantil, Penal y en las normas procesales, reclamando de todas ellas la reconceptualización de sus postulados doctrinales, y la adaptación de sus normativas ante las nuevas relaciones sociales y jurídicas, que se generan por la incidencia y generalización de las aplicaciones de dichas tecnologías en la sociedad, e incluso la regulación de nuevas realidades no previstas por el Derecho.

Pero, en mi criterio, el Derecho de la Informática no es sólo orden normativo, sino práctica jurídica y es también, por qué no, una comunidad doctrinal en búsqueda de nuevas soluciones. Estimo que está muy vinculado a una modernización del Derecho y por tanto es la gestación de un Derecho del porvenir que estamos necesitando en el hoy. Es transitivo con respecto a que muchas de sus instituciones ya paulatinamente se incorporan al acervo doctrinal y el devenir de las ramas tradicionales y en sí mismo por su objeto de estudio siempre está evolucionando y estudiando nuevos problemas, pienso que asistimos a un momento excepcional del desarrollo del Derecho y que podemos ser activos contribuyentes en su consolidación.

b)- ¿Dónde se encuentran las principales realizaciones?:

La protección de los Datos y la Información en general: Experiencias en Cuba y otros países latinoamericanos.

Como se sabe la información procesada por medios electrónicos o que circula por las redes no tiene iguales características, por lo que no se puede adoptar para ésta las mismas normas de protección. Generalmente existen dos grandes áreas de atención por parte del Derecho, las que alcanzan a un tratamiento muy especializado; por una parte, nos encontramos con los Datos Personales, y por otra, la información de carácter patrimonial, que es la que abarca

a los datos estratégicos de entidades, y la que está sujeta a las normas de propiedad intelectual siempre que sean creaciones reconocidas por sus dos regímenes jurídicos Derecho de Autor y Propiedad Industrial.

Alrededor de estas dos grandes áreas muy diferentes se han generado desde la década de los años 60, tanto pronunciamientos de la ONU, específicamente la Comisión de Tratamiento de las Minorías, y la adopción del Convenio de Estrasburgo, sobre "Protección de Datos Personales", así como la promulgación de legislaciones nacionales que ya alcanzan la tercera generación y cuya expresión más reciente es la Ley Orgánica de Protección de Datos Personales más conocida como LORTAD, de España.

En el caso de la Protección de los Datos Personales, considero que el origen lo podemos encontrar vinculado a la diversificación de las aplicaciones informáticas al tratamiento de la información personal, entiéndase cuentas bancarias, Registros Civiles, de Personal, de Actos de Ultima Voluntad, de Sancionados, entre otros; se inició en la década de los años 60 un movimiento de la doctrina jurídica y de la jurisprudencia de los países con mayor grado de desarrollo tecnológico tendente al reconocimiento del derecho a la libertad informática y a la autodeterminación en la esfera informativa, que tiene su principal instrumento de garantía en el Habeas Data, es decir en la facultad de las personas de conocer y controlar las informaciones que les conciernen y que están procesados en bancos de datos informatizados.

Las disposiciones legales surgidas como consecuencia del tratamiento automatizado de los datos personales, están destinados a proteger a los titulares de los datos: el individuo, ante los usos abusivos de información que pueden atentar contra los derechos fundamentales, es por ello que las leyes de Protección de Datos Personales, tienen un fuerte vínculo con el Derecho Constitucional, como por ejemplo, tanto en la Constitución española como en otras latinoamericanas se reconoce el deber de uso correcto de la informática y se instituye el Habeas Data, que no es más que un recurso procesal que se erige en garantía en el ejercicio de los derechos sobre la información.

Lo que se ha dado en llamar el Habeas Data, tal como lo ha definido el Dr. Antonio E. Pérez Luño, "constituye, en suma, un cauce procesal para salvar las libertad de la persona en la esfera informática" y cumple una función paralela en el seno de los derechos humanos de la "tercera generación", en

correspondencia con los que en los de la "primera generación" correspondió el Habeas Corpus respecto a al libertad física o de movimientos de las personas.

En latinoamérica, Brasil es el primer país que recogió este postulado en su constitución, más recientemente se han incorporados postulados en la de Perú y Argentina.

La destrucción, manipulación, adulteración o divulgación no autorizada de datos puede ser causada. básicamente, por problemas técnicos, desastres naturales y por seres humanos; son estos últimos los más comunes y que mayores preocupaciones tienen para aquel que tienen información o que tienen el deber de protegerlos de los peligros que semejantes eventualidades pueden producir.

Considero que el empleo razonable de los sistemas de información en interés de la sociedad, así como la protección segura de toda la información, son factores predeterminantes de una actitud de respeto por esta ciencia. En consecuencia, a la par de las aplicaciones informáticas haya que desarrollar valores éticos entre los sujetos vinculados a los sistemas. En tal sentido las normas jurídicas deben establecer claramente el régimen de disciplina informática.

En el caso de Cuba, desde el punto de vista institucional, se constituyó, desde 1988, un Grupo de Expertos de Protección de Datos, que más tarde se denominó Comisión Nacional de Protección de Datos, adscripta al Frente Nacional de la Electrónica.

Esta comisión estaba integrada por especialistas en Informática y en Derecho, los cuales tuvieron a su cargo estudiar y proponer las soluciones técnicas respectivas que se deban adoptar con el fin de garantizar la seguridad de los datos almacenados en los sistemas de información.

Así la comisión asesoró la promulgación por parte del Instituto Nacional de Sistemas Automatizados y Técnicas de Computación (INSAC), del Reglamento de Protección de Datos y Programas Informáticos; en el que quedaron establecidas las funciones de los responsables de la protección de datos y las medidas que se deben hacer cumplir en las entidades que procesen datos por medios informáticos.

A este esfuerzo de la Comisión se incorporó el apoyo decisivo de la UNESCO, para el coauspicio del Laboratorio Latinoamericano de Protección

contra Virus Informático, inaugurado el 11 de mayo de 1993; destinado al intercambio activo de información y productos detectores y descontaminadores de virus; además de ofrecer un marco propicio para el fomento de una cultura de protección y el trabajo técnico de desactivación y aislamiento de virus en el ámbito de toda la región iberoamericana.

Es menester señalar que este laboratorio tuvo como antecedentes inmediatos trabajos realizados en Nicaragua y México, en los que especialistas cubanos han ofrecido su experiencia y productos antivirus y en las jornadas desarrolladas en mayo de este año que dieron cabida a la materialización del Seminario Internacional de Protección contra Virus Informáticos, el Taller Práctico, y el Curso de Problemas Eticos y Jurídicos de la Información Automatizada, que sesionaron en el marco de la inauguración de esta importante institución.

Particular interés debe despertar al que lee estas notas el conocer que este Laboratorio de Protección contra Virus Informáticos tiene entre sus objetivos primordiales servir de centro de formación de profesionales vinculados a la Informática Jurídica en los temas de protección de la información, permitir el intercambio de experiencias legales en los diferentes aspectos que las nuevas tecnologías de la información le plantean al Derecho, así como propiciar la realización de proyectos de investigación relacionados con esta materia e incluso facilitar, en tanto centro coordinador, el intercambio de expertos entre los diferentes países.

Desde el punto de vista de las aplicaciones informáticas al Derecho, para el desarrollo de las políticas y estrategias que rigen la realización de proyectos vinculados a la actividad registral y documentaria que se llevan a cabo por los especialistas del Ministerio de Justicia de Cuba, se han tenido como bases las funciones y atribuciones de esta institución dentro de Sistemas de Organización de la Administración Central del Estado, establecidas por el Decreto Ley N° 67 de 19 de Abril de 1983.

La solución legislativa de protección de datos, abarcó además los regímenes de importación y exportación de productos informáticos, específicamente soportes magnéticos, por lo que las normas jurídicas de protección se hicieron extensivas a las normas de control aduanero.

Otro hecho relevante para Cuba y Latinoamérica en este área cada vez más urgente, dada la cantidad y peligrosidad creciente de los agentes contaminadores de los sistemas informáticos, fue la inauguración el 11 de mayo de 1993 del Laboratorio Latinoamericano de Protección contra Virus Informáticos, el que tiene entre sus objetivos fundamentales contribuir al noble empeño de fomentar en los sujetos vinculados a los sistemas informáticos una cultura y ética de utilización de las innumerables ventajas que la Informática como ciencia aporta a la humanidad.

- Protección legal del Software.

Al igual que en otros países, estuvimos al tanto y practicamos las diferentes vías de protección del software: Protección Industria, Derecho de Autor y una protección especial.

Hoy con la pertenencia de nuestros países a la Organización Mundial del Comercio, todos estamos inmersos en una actualización de nuestras leyes de Derecho de Autor, existen algunos pioneros dentro del área, pero también no se puede perder de vista las experiencias y prácticas desarrolladas en los entornos de esquemas de integración tales como MERCOSUR, NAFTA, Tratado de Libre Comercio y Pacto Andino.

- Contratación Electrónica y Contratos Informáticos.

Por este tema también se ha transitado, se ha legislado particularmentç en Argentina y en Venezuela, y también hay que estudiar el tema en el entorno de los esquemas regionales de integración.

Existen trabajos muy interesantes sobre el EDI.

Para la solución de conflictos se ha reconocido al Tribunal de Conciliación y Arbitraje de Mercosur. (TRICAMER)

En resumen se puede asegurar que existe un Derecho de la Informática en el área, algunos países como Brasil y México, han emprendido proyectos sistematizadores sobre el tema.

En Brasil desde el Ministerio de Ciencia y Tecnología, así como el Programa SOFTEL 2000.

En México desde la Cámara del Senado y el INEGI, a partir del Programa de Informática para el 2000.

c)- ¿Existe una comunidad intelectual en el área preocupada y ocupada en estos temas?:

Sí, existe y debe consolidarse aún más sobre la base de integrarnos en proyectos de investigación y en la búsqueda de soluciones prácticas en correspondencia con las características, tradiciones y realidades jurídicas, sociales y económicas de nuestra región.

Entre los principales centros de investigación, desarrollo y capacitación se encuentra el ILATID, en Argentina, fundado por el Dr. Antonio Millé, que desde hace muchos ha identificado a los problemas generados por la incidencia social de los avances tecnológicos como Derecho de Alta Tecnología.

Con otras realizaciones y orientados a otras áreas de conocimientos: aplicaciones informáticas al Derecho, hay que tener en cuenta: al CINADE, de Uruguay; el Instituto de Investigaciones Jurídicas de la UNAM; el Instituto de Informática Jurídica, de la Universidad Mayor de San Marcos, en Perú, a las experiencias de la Universidad del El Salvador, en Argentina y a la Facultad de Derecho de la Universidad de La Habana, entre otras muchas instituciones académicas, algunas de las cuales, como es el caso de ésta última que alcanza también al estudio del Derecho de la Informática.

d)- ¿Cuáles son las principales realizaciones en materia de Informática Jurídica?.

Atendiendo a la clasificación de las áreas de aplicación de la Informática Jurídica podemos hablar por ejemplo:

Informática Jurídica Documental:

El Sistema Argentino de Informática Jurídica, SAIJ;
El Sistema del Senado en Brasil, PRODASEN;
El Sistema del Congreso del Perú;
El Proyecto MENJUR, Cuba.

Informática Jurídica de Gestión y de auxilio a la toma de decisiones:

El sistema de Controlaría de Uruguay.

e)- ¿Cuál es la realidad y perspectiva de Cuba en las áreas de la Informática Jurídica y el Derecho de la Informática?.

En la actualidad nuestro país asiste a este extraordinario momento en que vive el planeta y se ha planteado un proceso de consolidación de la infraestructura nacional de la información: La Industria Nacional del Software y la Industria de los Contenidos de Información.

Como resultado de este proceso se ha comenzado a gestar un proceso de integración del Derecho en Cuba que exige la evaluación constante de la eficacia social de las normas preexistentes al fenómeno info-telemático y la generación además de nuevas disposiciones, lo cual ya va conformando un segmento del orden legal que reúne en su seno más de 30 disposiciones de diferentes rangos y materias (leyes, decretos leyes, decretos y resoluciones) e incluso la exigencia de adopción de Códigos Eticos por parte de los profesionales vinculados a estas actividades.[2]

También se ha transitado hacia una organización institucional que responda a la infraestructura de la información y que establece la constitución del "Registro de Redes", el "Registro de Distribuidores de Información Electrónica" y el "Registro de Dominios IP", por solo citar algunos ejemplos.

Lo anterior está íntimamente relacionado con la decisión de nuestro país de emprender "Proceso de Informatización de la Sociedad Cubana" en víspera del próximo milenio.

En correspondencia con ello, ya nuestro Estado viene trabajando en el proyecto de documento programático que debe implementar la política trazada, todo lo cual ha sido expresado en el Documento "Lineamientos estratégicos de informatización para el año 2000".

■[2] Correa y otros, "Derecho Informático", pág. 230. Ediciones Depalma, Buenos Aires, 1987.

El ámbito de la Informática Jurídica se viene trabajando en la consolidación de varios proyectos de informatización de los principales Registros: Civil, Actos de Ultima Voluntad, Central de Sancionados. También en un Banco de Datos sobre resoluciones judiciales e instrucciones del Tribunal Supremo Popular. Algunos resultado se han alcanzado en la Fiscalía General de la República. También trabaja en sistemas de información jurídica automatizada (doctrinal y legislativa).

f)¿Cómo acercarse a la realidad de nuestro área para conocerla, intercambiar e integrarnos en la investigación?.

Existe desde el año 1984 un foro sistemático para conocer la realidad de Iberoamérica en estos temas: los Congresos Iberoamericanos de Derecho e Informáticos que tiene como antecedente el I realizado en Santo Domingo, a los que les han sucedido los de Guatemala (1989), Mérida (1992), Bariloche (1994) y La Habana (1996), de los que en sus Actas se recoge un devenir práctico y conceptual sobre todos temas de la mutua incidencia del Derecho y las Nuevas Tecnologías de la Información y la Comunicación.

## II. RESPONSABILIDAD PENAL DERIVADA DEL USO INDEBIDO DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN: ¿DELITOS INFORMÁTICOS?.

La destrucción, manipulación, adulteración o divulgación no autorizada de datos puede ser causada, básicamente, por problemas técnicos, desastres naturales y por seres humanos; son estos últimos los más comunes y que mayores preocupaciones tienen para aquel que tiene información o que tiene el deber de protegerlos de los peligros que semejantes eventualidades pueden producir.

Como se ha dejado sentado, la Informática no es un fenómeno exclusivamente tecnológico con implicaciones estrictamente positivas. Sus efectos dependen del uso que se les dé. Las computadoras, al permitir un manejo rápido de grandes volúmenes de información, facilitan la concentración y disponibilidad automática de datos de diversa índole, lo que condiciona la necesidad de regular su protección desde el punto de vista de su uso y conservación.

Lo que se ha dado en llamar el dato electrónico, hoy más ya es más adecuado hablar de información digitalizada, debe ser protegido contra factores de riesgo tanto objetivos y subjetivos. Estos últimos generados por conductas

negligentes, culposas o inexpertas, las que condicionan la posibilidad de pérdida, alteración, sustracción o uso inadecuado de la información almacenada en soportes magnéticos o producir alteraciones en el funcionamiento de los sistemas informáticos, llegando a producir incluso un colapso en una actividad bien sea de servicios o productiva.

A menudo se escucha hablar de los perjuicios causados por los virus informáticos, de la práctica ilícita en torno a los sistemas automatizados que tipifican conductas de "fraude", "sabotaje" o "robo" de la información, o de programas "piratas" que penetran en las redes computarizadas y logran destruir o alterar los datos o programas incluso los medios técnicos.

En este segmento del problema me detendré a exponer más detenidamente, por lo que necesariamente me referiré a aspectos "históricos" del tema hasta nuestros días, específicamente con motivo de las II Jornadas del Delito Cibernético, realizadas en Mérida, entre los días 20 a 22 de noviembre.

II.(a) - Algo que ya es historia.

Desde sus orígenes, en 1890, cuando Herman Holleriht inventó un sistema capaz de realizar tabulaciones y, decisivamente, cuando en 1954, se comercializó por primera vez un microprocesador, el hombre se ha empeñado en ofrecer soluciones a los problemas de velocidad, volumen, capacidad y coste de la información.

Así, gracias a los estudios y aplicaciones de los circuitos integrados de silicio, ha logrado una velocidad de procesamiento más de 2000 veces superior a los primeros ordenadores, y reducir su costo en más de 25 veces.

No obstante, la propia complejidad de la técnica impone nuevos límites físicos, tecnológicos y económicos, y el hombre se ha dedicado a buscar soluciones basado en estudios de nuevas aleaciones mecánicas, memorias ópticas, células de memoria tridimensional, que marcan el presente y futuro de la Informática, y que se refleja en todo cuanto está, asociado a las partes físicas de la computadora (hardware), lo que alcanzó también al software, mientras éste era parte indisoluble de las unidades centrales de procesamiento.

Con el desarrollo independiente de la parte lógica (software), se varió este estado de correspondencia y entraron a jugar determinantemente otros factores.

En estos momentos el software es un elemento tan importante o más que las propias computadoras y en el que se han destinado fuertes inversiones al desarrollo de implicaciones y programas al servicio del hombre.

Producto de este vertiginoso desarrollo, hoy se cuenta con programas accesibles y de fácil utilización, pantallas de contacto, teclados y lenguajes sencillos, que han hecho posible la diversidad de aplicaciones informáticas así como el manejo y acceso cada vez más masivo y menos especializado a las técnicas de información.

Unido a este devenir de desarrollo tecnológico, la humanidad ha ido identificando un cambio en los paradigmas en cuanto al soporte de informaciones, pero ninguno ha sido tan trascendental como los que son fruto de la Revolución Informática, hito en el desarrollo social a partir de la cual se comienza a gestar lo que hoy se conoce indistintamente como "Sociedad de la Información" o "Sociedad del Conocimiento" e incluso algunos la identifican como la "Era digital", en cualquiera de ellas encontramos que en el vértice de todas estas realizaciones y como piedra angular sobre la cual se erige la información.

Por eso una de las características de este fin de siglo, denominado "La era de la Información" son, por una parte, la explosión de la información y, por otra, el desarrollo de nuevas tecnologías de información y comunicación. Estas últimas, permiten con facilidad desconcertante y apenas inimaginable, almacenar, recuperar y diseminar la información.

Por tal motivo se le reconoce a la Informática cuatro características las cuales están en directa relación con el efecto multiplicador que ha producido en las actividades económicas y sociales; particularmente en el aumento de la productividad técnica. La primera y principal característica son de permitir mayor velocidad de cálculo que aquella realizada por el hombre. La segunda característica, relacionada con la primera, es la de asociación y relación lógica. Una tercera es la relativa a la memorización, es decir, al almacenamiento de datos,

informaciones, imágenes y sonidos; y una cuarta, es la relativa a la posibilidad de ampliar la comunicación de estos datos, informaciones, imágenes y sonidos.[3]

Pudiéramos decir, además, que estas cuatro características sirven de pauta, además, para dividir metodológicamente esta era de la información, desde la informática en búsqueda de más posibilidades de almacenamiento de información, hasta la informática interactiva en la que estamos inmersos.

Pero la Informática no es un fenómeno exclusivamente tecnológico, con implicaciones estrictamente positivas. Junto a las ventajas que reportan los avances tecnológicos en la información, se manifiestan puntos débiles, problemáticos y riesgos que no eramos capaces de imaginar.

Con estos avances tecnológicos, se han introducido nuevos soportes de datos de dimensiones reducidas, que no sólo son fáciles de ocultar, sino que resulta común su trasiego, con el fin de intercambiar datos y programas.

Esta tecnología ha obligado a reestudiar y crear nuevos mecanismos para proteger la información, los cuales se complican cada vez más, si analizamos que en un inicio se limitaban quizás a un centro de cálculo cerrado, pero ahora se ha extendido al uso de las máquinas interconectadas tanto nacional como internacionalmente, a través de líneas telefónicas.

Por lo que podemos afirmar que el impacto social de las nuevas tecnologías y sus efectos dependen del uso que se les dé.

De ahí que a finales del siglo XX, el balance del desarrollo de la Informática exhiba enormes posibilidades y aciertos, como efectos indeseables. Uno de ellos lo constituyen las manifestaciones de uso indebido de las nuevas tecnologías de la información y la comunicación[4].

■[3] Carlos Ferreyros, "Aspectos metodológicos del delito informático", Notas del curso Nuevas Tecnologías y Derecho, UNED, mayo de 1995. Mérida, España.

■[4] Antonio Enrique Pérez-Luño, "Impacto social de la nuevas tecnologías" pág. 15 Editorial Fundesco, 1987.

La magnitud de los daños[5], es un fenómeno que ha quedado, podemos decir en sentido general, fuera de las legislaciones, pues hasta estos momentos no existe de modo integral un sistema de normas que proteja específicamente a los datos computarizados contra robo, desvío, daño, alteración, destrucción, acceso indebido u otras acciones que afectan de alguna forma la información que se procesa por medio de esta tecnología.

Dichas conductas, tienen su origen desde el propio surgimiento de las aplicaciones informáticas y a pesar del nivel de desarrollo de la sociedad e incidencia de afectaciones en múltiples bienes tutelados o tolerables jurídicamente, aún existe una pobre presencia de respuestas legales a tales actos indebidos.

Muchos autores al tratar el tema, hablan de "Delitos Informáticos", refiriéndose en forma genérica a todas aquellas acciones en que los sujetos se valen de la Informática para realizar sus actos.

En la actualidad, existen dos realidades latentes, algunos códigos penales y leyes especiales –pocos- que recogen en forma de tipos penales, dichas conductas y en cuyo caso puede hablarse propiamente de "delito". Y otra realidad - la más generalizada -, la constituyen las manifestaciones de conductas que valiéndose de las computadoras como medio o fin, transgreden un orden legal establecido o causan un daño, pero no constituyen delitos por no estar tipificadas como conductas antijurídicas en un cuerpo legal, rigiendo en estos casos el principio de nullum pena sine previe llegue penal.

De modo que ante el tema, expresión del impacto negativo de las nuevas tecnologías de la información y la comunicación en la sociedad, por el momento y al parecer aún por un rato, siempre nos estaremos refiriendo, a conductas típicas y a conductas atípicas.[6]

■[5] Se estima que las pérdidas de información, oscila anualmente entre los US$ 3 y 5 millones. Esto en una empresa grande; en una empresa pequeña, la pérdida de información puede significar el fin de su existencia.

■[6] Julio Téllez Valdés, "Derecho Informático", pág. 81. Editorial Instituto de Investigaciones Jurídicas, Serie A: Fuentes, b) texto y estudios legislativos, No. 75. No. 75.

En lo particular, preferimos no hablar de delito para aludir a un comportamiento no tipificado como tal en un cuerpo normativo, por tal motivo hemos preferido al titular este trabajo, en tales supuestos, referirnos a actos indebidos.

Aunque de inicio también hago explícita mi posición en cuanto a compartir el criterio que en la inmensa mayoría de los casos se está en presencia de viejos delitos cometidos por medio de nuevas tecnología. Afortunadamente estas posiciones van ganado espacio en la realidad jurídica en el ámbito mundial y presiento una especie de madurez intelectual y práctica al abordar el tema, dejando de un lado las primeros tendencia de "adjetivación de informático a las nuevas manifestaciones de actos indebidos", no obstante pienso que estamos en el deber de agradecer a los pioneros de estas posiciones y prácticas el haber contribuido al desarrollo, aún no consolidado, de las tendencias más modernas de legislar y enfrentar el tema, tanto desde la instrucción como desde el Derecho.

III.(b) - Dimensión del Problema.

Como se conoce los sistemas informáticos a menudo se utilizan para almacenar datos políticos, económicos, médicos, sociales y personales muy delicados y ofrecen posibilidades ilimitadas de concentración y manejo de información.

La información que se elabora automáticamente y se archiva en las computadoras, es algo vivo, cambiante, dinámica y directamente relacionado con la vida humana en todas las esferas de la sociedad y constituye hoy en día, uno de los patrimonios más valiosos.

En la actualidad la información ha adquirido características de bien social, económico y jurídico autónomo. En cuanto a su forma, se ha separado de su continente tradicional: el paradigma papel, que hoy convive con el soporte digital; sin embargo la información se ha independizado de los mismos sin perder su identidad y su función.

Por otra parte, a la información se le reconoce valor como materia prima fundamental en el cuarto sector industrial. Se identifica además, como un recurso estratégico para el desarrollo; de manera tal, que los cambios estructurales son

palpables en términos de indicadores de crecimiento económico, ya se comienza a distinguir entre países inforricos e infopobres.

También se reconoce, que la aplicación de las nuevas tecnologías de la información y la comunicación al entorno social en general es fuente de un sector productivo en tanto genera bienes y servicios y modos diferentes de realización del comercio internacional.

El uso de estas nuevas tecnologías ha generado importantes beneficios en el tratamiento de los datos; sin embargo, tales beneficios constituyen a la vez un motivo de preocupación, pues la informatización ha resultado otra posibilidad de realizar actos indebidos.

Las acciones generadas en el manejo de las técnicas de computación han sido consideradas como conductas delictivas en el contexto del desarrollo; lo que evidencia la interdependencia entre el nivel de evolución tecnológico, el grado de desarrollo económico y social y la manifestación de tales conductas.

El empleo indebido de dichas técnicas o los atentados contra su integridad y funcionamiento de los sistemas automatizados de información, constituyen o puede constituir una agresión a múltiples intereses, tales como la vida de las personas, los derechos humanos, las libertades fundamentales y la soberanía e independencia de los Estados.

El peligro de que tales hechos se produzcan, se acrecienta cada vez más con la multiplicación de todas las aplicaciones en forma de redes informáticas, lo cual es posible gracias al desarrollo e integración de las técnicas informáticas y de telecomunicaciones, conocido como Telemática.

Con el desarrollo de los sistemas telemáticos, tales como transmisión de datos en paquetes y el correo electrónico, se amplía el horizonte de la acción transgresora, al facilitarse que el hecho que se produzca sea contrario al orden social o jurídico de más de un país; de manera que estos actos indebidos constituyen, además, un reto para el Derecho Internacional, cuando la acción transgresora afecta a más de una jurisdicción nacional.

Sin duda alguna, las manifestaciones de actos indebidos generados por el mal uso de las técnicas informáticas constituye uno de los más complejos y preocupantes fenómenos surgidos de la interacción hombre-máquina.

La complejidad del tema está dada por la propia naturaleza de la Informática, la amplitud y profundidad del avance tecnológico de las técnicas de comunicación y su incidencia en todas las esferas de la vida humana, lo que la ha hecho portadora de profundos cambios en nuestras formas de conductas y modos de pensamientos.

Es una preocupación, porque, ante su manifestación la sociedad en general se encuentra doblemente desarmada; bien sea por la ausencia de una legislación especifica en materia de Informática, o la insuficiencia de las fórmulas legales tradicionales para subsumir en ellos las nuevas formas de instrumentación de la acción, o porque, aún en los casos de tipificación especifica, no están preparados sus órganos de represión y justicia en el manejo técnico necesario para comprender y enfrentar a los sujetos de estas acciones.

A la vez, la falta de una legislación especifica y la escasa preparación del personal de los cuerpos de seguridad del Estado, son factores que en cierta medida han condicionado el grado de proliferación de éstas conductas.

Pero, al parecer, aún no existe una conciencia general de esta relación causa-efecto, pues a la par del desarrollo tecnológico continúan presentes el silencio jurídico y grandes áreas de desrregularización.

Si la informática supone una actividad y ésta se manifiesta en muchos de los ámbitos del quehacer humano es necesario regularla por el Derecho.

Regular todas las actividades relacionadas con la informática en general y con las tecnologías relacionadas con ésta, supone establecer normas jurídicas que fijen un marco regulatorio tanto con relación a las actividades y creaciones informáticas; como la regulación de conductas jurídicas; derechos y obligaciones relacionadas con la Informática.

Pero el horizonte ya empezó a cambiar y se comienza a hablar en el seno de Naciones Unidas de comenzar a trabajar a favor de un marco regulatorio fruto de la colaboración y armonización de nuestras legislaciones nacionales y especialmente de la voluntad de enfrentar coordinadamente esta realidad. Cierto es que es un camino difícil pero transitable.

Por otra parta también ya desde hace algún tiempo la comunidad intelectual viene trabajando en el tema. Sobre el decursar de ambas rutas y con la esperanza de que algún día converjan me referiré a continuación a algunas cuestiones más bien de derecho positivo, otras de hechos; otras de líneas de pensamientos que comparto.

## IV. DELITO INFORMÁTICO: ESPECIFICIDAD Y COMPLEJIDAD.

Asistimos a la conceptualización del fenómeno por lo que las referencias que a continuación se relacionan no se deben entender como definitivas, sino más bien son intentos de explicación de tales acciones.

Algunos ejemplos de conceptos constituyen una tipificación legal propia y están contemplados en leyes y códigos penales; otros son citas puramente doctrinales.

Según la Organización para la Cooperación Económica y el Desarrollo (OCDE) delito informático es "Abuso informático, y es cualquier acto ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos".[7]

El Departamento Norteamericano de Justicia ha definido delito informático como cualquier acto ilegal para el que es esencial el conocimiento de la tecnología informática para su comisión, investigación y persecución.

Según Correa "delito informático es toda acción dolosa, que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos utilizados en las actividades informáticas".[8]

■[7] OCDE: Manual de las Naciones Unidas sobre el Desarrollo y Control de Delitos Informáticos, 1994.

■[8] Correa y otros, "Derecho Informático", pág. 230. Ediciones Depalma, Buenos Aires, 1987.

Para el destacado penalista italiano Carlos Sarzana, delito informático es "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".

Para la Dra. María de la Luz Lima, es el "Conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiéndose presentar múltiples formas de lesión de variados bienes jurídicos".

Por su parte Luis M. del Pont y Abraham Nadelsticher, lo consideran como "toda acción típica, antijurídica y culpable, pero cuya conservación se usa la tecnología computacional o se afecta a la información contenida en un sistema del tratamiento automatizado de la misma".[9]

El destacado jurista costarricense Juan Diego Castro, reconoce que delito informático es "aquel hecho en el que el que independientemente del perjuicio que pueda causarse a otros bienes jurídicamente tutelados y que eventualmente pueden causar en forma real o ideal y se atacan elementos puramente informáticos."[10]

Sin embargo algunos tratadistas como Parker 1985; han intentado definirlo como "Todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio".[11]

Otros se circunscriben al aspecto patrimonial del problema y lo definen como el "Conjunto de acciones dolosas que provocan un perjuicio a personas físicas o entidades, sin que sea necesario que ello conlleve un beneficio material para su autor, o viceversa, produce un beneficio ilícito para su autor aun cuando no perjudique de forma ostensible a la víctima".

■[9] Luis M. del Pont y Abraham Nadelsticher, "Delitos de Cuello Blanco". Cuaderno No. 8 del Instituto Nacional de Ciencias Penales (INACIPE), México, 1981.

■[10] D. B. Parker, "Combatte la criminalité informatique". París, Editorial Oros, 1985.

■[11] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

Dirk Hanson, en su articulo "Los nuevos alquimistas" dice que delito informático es "una forma de irrumpir y penetrar en los que herramientas del ladrón son, en esencia, un conocimiento de la estructura lógica o los puntos lógicos débiles inherentes a un sistema particular de programación y proceso. Más allá de un conocimiento profundo de la programación, las únicas herramientas que el forajido necesita son un terminal de ordenador y teléfono. No tiene que acercarse en absoluto al escenario del crimen".

Por su parte, Klaus Tiedmann, en Criminalit da Computer, dice: "cometer delito informático la persona que maliciosamente use o entre a una base de datos, sistema de computadoras o red de computadoras o al cualquier parte de la misma con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información".

Para el autor, también comete este delito "el que maliciosamente y a sabiendas y sin autorización intercepta, interfiera, recibe, usa, altera, daña o destruye una computadora, un sistema o red de computadoras o los datos contenidos en la memoria, base, sistema o red".

De manera tal que "no existe una definición que esté reconocida en el plano internacional, lo corriente ha sido ahora que se utilicen definiciones funcionales", tal como apunta un informe de la OCDE " Manual de las Naciones Unidas sobre prevención y control de Delitos Informáticos" (1994).

A1 profundizar en las definiciones expuestas, éstas resultan igualmente vagas, ya que necesariamente tiene que entrar en la descripción de hechos o acciones diversas en móviles, sujetos y bienes jurídicos atacados, todo lo cual apunta tal como lo han considerado muchos estudiosos del tema, a las hipertrofias de los ordenamientos penales que así lo han considerado.

Sin embargo la expresión "Delito Informático" nos motiva además otros comentarios, ya que tal denominación a nuestro juicio resulta literalmente confusa, al parecer Informático califica al género y no a la especie, por eso consideramos que en todo caso serían Delitos contra la Informática, además se trata de una multiplicidad de conductas que se pueden generar que tienen en común utilizar las nuevas tecnologías de la información y la comunicación como medio para cometer el hecho.

No obstante, se habla y se seguirá hablando de los delitos informáticos como término que engloba a dichas acciones, e incluso propio de un tipo de delincuencia.

En términos de tipificación de conductas los especialistas generalmente coinciden en reconocer como delito acciones de fraude informático, falsedad informática, sabotaje informático, acceso no autorizado, interceptación no autorizada, reproducción no autorizada de un programa protegido, reproducción no autorizada de una topografía, los delitos de alteración de datos o programas, espionaje informático, y utilización no autorizada de un equipo informático o de un programa.

La primera tipificación de delitos perpetrados por computadoras o sobre soportes informáticos fue realizada por Lampe en 1975, quien al decir de Sieber, responde, no sólo a un criterio de sistematización vinculado a la característica del procesamiento de datos, sino al mismo tiempo a una separación de diversos tipos criminológicos de conductas.

Primero Lame y más tarde Sieber proponen los siguientes tipos delictivos: fraude por manipulaciones de un computador contra un sistema de procesamiento de datos.

Fraude informático, constituye la forma más frecuente de aparición de conductas desválidas en las sociedades de alto desarrollo tecnológico y constituyen el núcleo criminológico de los llamados "delitos informáticos".

Consiste en el cambio de datos o informaciones ya contenidas en la computadora en cualquier fase de su procesamiento o tratamiento informático, en el que media ánimo de lucro y genera perjuicio a terceros

b) espionaje informático y robo de software.

Es la obtención ilegal de información mediante medios informáticos para su utilización en actos posteriores en el que se busca satisfacer un interés, el cual tiene efectos económicos de gran magnitud.

c) sabotaje informático.

Destrucción o inutilización de datos o programas informáticos dirigidos a causar un perjuicio sobre bienes patrimoniales, tanto para el titular como al usuario del sistema.

O los que se realizan con finalidad política actuando contra la seguridad y defensa de los Estado al dirigir sus actos nocivos a la destrucción o inutilización de sistemas de información sobre armamentos, organización operativa de las fuerzas armadas o ficheros de la policía.

d) robo de servicio.

Robo de tiempo de máquina. Utilización indebida del equipo informático o de los servicios de procesamiento de datos; bien sea en sito o a través de acceso remoto del que puede resultar la obtención ilegal de información.

e) acceso no autorizado a sistemas de procesamiento de datos.

f) ofensas tradicionales en los negocios asistidos por computador.

g) uso de un equipo propio para defraudar o enmascarar acciones punibles.

Otros autores, como el Dr. Julio Téllez, profesor del Instituto de Investigaciones Jurídicas de la UNAM, de México, lo clasifican atendiendo a dos criterios: como instrumento o medio y como fin u objeto, al proponer los supuestos siguientes: Supuestos en que se utilizan las nuevas técnicas como medio u objeto. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques). Variación de los activos y pasivos en la situación contable de las empresas. Planeación o simulación de delitos convencionales (robo, homicidio, fraude). "Robo" de tiempo de computadora. Lectura, sustracción o copiado de información confidencial. Modificación de datos, tanto en la entrada como en la salida. Simulación de servicios no rendidos.

Aprovechamiento indebido o violación de un código para penetrar a un sistema, introduciendo instrucciones inapropiadas.

Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria específica, método conocido como técnica de salami.

Uso no autorizado de programas de cómputo.

Introducción de instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios.

Alteración en el funcionamiento de los sistemas.

Obtención de información residual impresa en papel o cinta magnética luego de la ejecución del trabajo.

Acceso áreas informatizadas en forma no autorizada.

h) Intervención en las líneas de comunicación de datos o teleproceso.

Supuestos en que las nuevas técnicas constituyen el fin u objeto del acto indebido.

Programación de instrucciones que producen un bloqueo total al sistema.

Destrucción de programas por cualquier método.

Daño a la memoria.

Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales).

Sabotaje político o terrorismo en que se destruye o surja un apoderamiento de los centros neurálgicos computarizados .

Secuestros de soportes magnéticos en los que figure información valiosa con fines de chantaje o el pago de rescate, entre otros.

Entre los años 1985 y 1989, un Comité Especial de Expertos sobre delitos relacionado con el empleo de computadoras, del Consejo de Europa, se dieron a la tarea de examinar los problemas jurídicos que planteaban los delitos informáticos.

El resultado de este trabajo se conoció en forma de Recomendación que suscribieron el Comité especial y el Comité Europeo para los Problemas de

Delincuencia, que el Consejo de Europa aprobó el 13 de septiembre de 1989, Recomendación N° R (89)9.

Las directrices del Consejo de Europa recogen:

" 1. Lista mínima de los delitos reconocidos normativamente y entre los cuales enuncia a los siguientes:

a) Fraude informático.

b) Falsificación informática.

Daños ocasionados a datos de computadoras.

- Sabotaje informático.

- Acceso no autorizado.

- Intersección no autorizada.

- Reproducción no autorizada de un programa de computadora protegido.

- Reproducción no autorizada de una topografía".

"Lista facultativa que contiene las formas de conductas siguientes:

- Alteración de datos de computadoras o de programas de computadoras.

- Espionaje informático.

- Utilización no autorizada de una computadora.

- Utilización no autorizada de un programa de computadora protegido".

En el informe de la OCDE que ya aludimos con anterioridad se presenta también una lista de propuestas de sistematización de conductas generadas del uso indebido de tecnologías de información y comunicación sean éstas como objeto de delitos o como instrumento para cometerlo.

Al relacionarlas el Informe reconoce que los supuestos que a continuación relacionaremos resultan ser los que más comúnmente se han presentado:

"Manual de las Naciones Unidas sobre prevención y tratamiento de los Delitos Informáticos":

Tipos comunes de delitos informáticos.

- Fraudes cometidos mediante manipulación de computadoras.

- Falsificaciones informáticas.

- Daños o modificaciones de programas o datos computarizados.

- Acceso no autorizado a servicios y sistemas informáticos.

- Reproducción no autorizada de programas informáticos de protección legal".

Las relaciones taxativas de supuestos de actos indebidos siempre quedan incompletas, y además se identifican con figuras delictivas convencionales vigentes en nuestros Código, lo cual no siempre es conveniente para comenzar a estudiar el problema, pero sin lugar a dudas dan medida de la diversidad de sus manifestaciones, las que están íntimamente relacionadas como ya dijimos con anterioridad con la multiplicidad de aplicaciones informáticas.

No obstante consideramos que la propuesta de la OCDE en sí mismo constituye un primer intento de sistematización del fenómeno de la tipología y una importante contribución a la estandarización en el tratamiento del mismo fenómeno, especialmente si consideramos que estamos ante conductas típicas de una delincuencia sin fronteras.

El debate doctrinal se desarrolla en varias direcciones. Algunos especialistas consideran que algunos supuestos no son otra cosa que modalidades de un mismo tipo delictivo, otros estiman que no todas las conductas pueden ser enmarcadas como delitos informáticos en el sentido de una nueva forma de un nuevo tipo de tipología, tal es el caso de la reproducción o utilización no

autorizada de un programa o de una topografía de semiconductores, éstos considerados, como delitos contra la propiedad intelectual o industrial.

Por su parte, otros creen que supuestos tales como los de fraude informático, falsedad informática o espionaje, son modalidades de delitos reconocidos por la doctrina penal, en los que el uso del sistema informático no es otra cosa que el medio de comisión.

Y no faltan los que plantean que la novedad de la acción está en que el bien afectado son los recursos informáticos.

Tal es el caso que la acción recae sobre los elementos físicos donde se pueden dar manifestaciones típicas de hurto, robo o apropiación indebida del equipamiento o parte de éste, incluso la inutilización o destrucción de los mismos, por lo que no estaríamos en presencia de nuevas conductas sino de acciones delictivas a las que le son aplicables las reglas propias de la legislación ordinaria.

Otro supuesto puede ser la destrucción, menoscabo o inutilización de los elementos fiisicos los que podrían subsumirse en las figuras de estragos y daños.

Particular análisis merece el hurto de tiempo de máquina el que se considera un caso atípico como tal hurto de uso.

Ahora bien, cuando se atenta contra el software y la acción recae sobre la información o conjunto de datos almacenados en soportes magnéticos, sin que resulte alterado alguno de los elementos del Hardware, o por lo menos sin que sea necesaria dicha alteración física, aunque pueda ocurrir; entonces el tema merece otro comentario.

Pienso que las acciones sobre el software, por la propia naturaleza de éste -intangible- son las que más interrogantes por no decir las únicas, ofrecen al Derecho.

Un caso, el apoderamiento de ficheros informáticos, en la que la acción puede ser la copia sin destrucción del original.

Tal conducta genera un sinnúmero de situaciones para subsumir el acto en un tipo legal convencional, ya que la sustracción del fichero no conlleva la

acción "tomar o apoderarse" en el sentido literal y jurídico de la definición, tal supuesto es sólo válido en caso de sustracción de soportes magnéticos.[12]

En sentido general tanto de las definiciones como de las tipificaciones de tales actos indebidos podemos extraer varios elementos comunes, las que a su vez están relacionadas con los factores de vulnerabilidad consustanciales a los sistemas informáticos.

A nuestro juicio entre los factores que propician tales conductas y los rasgos comunes que están presentes en la generalidad de ellas se encuentran las siguientes:

- Son conductas diversas que se manifiestan a través de una gama de actos específicos con características muy peculiares, lo cual está dado por la diversidad de aplicaciones informáticas las que abarcan casi todas las esferas sociales por lo tanto íntimamente relacionado con dos factores: densidad de la información y procesos, así como la vulnerabilidad electrónica.

- Ilegales; los sistemas aplicaciones y servicio informático legítimo deben estar realizados en correspondencia con los principios legalmente reconocidos y ajustados a las normas técnicas internacionalmente reconocidos (ISO/9000).

- No éticas; entre las implicaciones sociales de la incidencia de las nuevas tecnologías de la información y la comunicación se encuentra la generación y el fomento de nuevos valores éticos y la adopción de códigos deontológicos. La infracción de las reglas del deber ser siempre está presente en estas conductas.

- Agreden tanto al elemento físico como al lógico de los sistemas de información, lo cual está sustentado en la condición de vulnerabilidad de los medios electrónicos de procesamiento de datos.

- Se utilizan los sistemas informáticos como medios o fin del acto; lo que se corresponde con las reglas de accesibilidad indispensable para el uso de sistemas.

■ [12] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

- Atacan varios bienes jurídicos, a veces los propios medios informáticos, ello está derivado tanto de la densidad de la información y procesos, como del factor de vulnerabilidad electrónica presente en toda aplicación informática o telemática.

- Su descubrimiento bastante dificultoso, de altísimo costo económico; lo que está fundamentado en la complejidad de los propios medios o sistemas atacados o utilizados para cometer la acción y el factor humano imprescindible para la materialización de los hechos.

- Los autores operan en condiciones de máxima seguridad, en virtud de estar amparados por conocimientos técnicos fuera del alcance de cualquier individuo no especializado, este supuesto se fundamenta también en la conjugación de dos factores: de complejidad y elemento humano.

Por otra parte, estas conductas suscitan problemas respecto a la determinación de la autoría, la delimitación del inter-crimen y la valoración del perjuicio.

En sentido general, la tipificación de estas acciones requiere la determinación de un sujeto específico.

En muchas ocasiones estas acciones se cometen en el desempeño de las funciones laborales[13], lo que evidentemente es otra característica que pone de manifiesto además los móviles que impulsan al comisor a incurrir en estas acciones.

También es propio, en la manifestación de estas conductas, el hecho de que el sujeto se aprovecha de una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico en que se manifiesta la acción[14]. Al sujeto en muchos casos le motiva demostrar cuan vulnerable es el sistema.

■ [13] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

■ [14] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

Las acciones de vulnerabilidad de sistemas de información no son nada vulgares, por el contrario se caracterizan por ser sumamente sofisticadas, y donde su mismo carácter técnico, dificulta mucho los actos de comprobación.

En un alto número, no se manifiesta la intencionalidad del autor, y muchas acciones se llegan a realizar por imprudencia.

Debido al uso frecuente y casi natural de las modernas técnicas de computación por parte del público infantil y juvenil, muchas de estas acciones pueden ser cometidas por menores, para los que el acto en sí constituye un juego o una reafirmación.

En otras ocasiones, personas mayores, conscientes del daño que ocasionan o del beneficio que pueden obtener, realizan sus fechorías en auxilio de menores.

Otro de los elementos que se manifiesta en estos casos, es que el comisor del delito no requiere estar presente en el lugar de los hechos ya que la manipulación de los medios necesarios para realizar su acción le permite hacerla a distancia.

Por tal razón el "Manual de las Naciones Unidas sobre la Prevención y Control de los Delitos Informáticos" en su párrafo acerca de las compilaciones debidas al carácter internacional del problema apuntó:

"Las fronteras nacionales, que en el pasado quizás obstaculizasen las actividades de los criminales, han desaparecido prácticamente con la llegada de las telecomunicaciones modernas. Para reunir las pruebas, los investigadores tienen que ser capaces de percatarse y ocuparse de cuestiones internacionales como la extradición y la asistencia recíproca. Al efectuar investigaciones internacionales hay que tener en cuenta los requisitos en materia de pruebas, procedimiento penal y protección de datos que se hallen vigentes en otras jurisdicciones".

De manera que, tal como alude el Manual de referencia: "El elemento internacional en la perpetración de delitos informáticos plantea nuevos problemas y nuevos retos para la ley. Es posible que se tenga acceso a un sistema en un país, que se manipulen los datos en otro, y que las consecuencias se dejen sentir en un tercero. Los datos informáticos pueden operar materialmente en un país, desplazarse electrónicamente a través del mundo, yendo de una red a otra, y

obtener fácilmente acceso a bases de datos situadas en un continente diferente. El resultado de todo esto es que hay que tratar con soberanías, jurisdicciones, leyes y normas diferentes. Más que en el caso de cualquier otro delito internacional, (la velocidad, movilidad, flexibilidad, importancia y valor de los delitos informáticos, la determinación del locus delicti (lugar del delito) influirá en la capacidad de un país determinado para castigar el delito. ¿Se basará la sanción en la jurisdicción territorial y en el derecho nacional, o habrá que aplicar principios extraterritoriales?".

Pueden ser víctima de estos actos cualquier persona individual o colectiva: bancos, compañías de seguros, servicios postales, organizaciones de seguridad social, bancos de datos de asistencia médica.

En los supuestos de entidades bien sean publicas o privadas, serán particularmente propicias aquellas instituciones con escaso o nulo nivel de seguridad informática.

También pueden ser víctimas titulares y demás beneficiarios legítimos de los sistemas informáticos ya sean usuarios directos o terceros.

Conjuntamente con su manifestación en la sociedad se genera un lenguaje en términos y modalidades propias que hacen más difícil su detección y comprensión para quienes no son especialistas en el área de informática.

Entre otros elementos que gravitan sobre el llamado delito informático haciendo más difícil su detección y sanción, es el hecho de que un elevado número de casos es descubierto al azar, ya sea por tratarse de situaciones no previstas por los mismos técnicos de seguridad, o por la inobservancia de las normas de seguridad por parte de los usuarios del sistema.

En las condiciones en que se operan estas acciones se dificulta la identificación de los autores, permitiéndoles a éstos gozar de los beneficios en absoluto grado de impunidad.

Al supuesto anterior se suma en que un alto porcentaje de casos descubiertos no son denunciados por distintas razones, entre otras, dificultad de detectar estas conductas debido a las condiciones y rapidez en que pueden ser manifestadas, las dificultades técnicas para probar el cuerpo del delito y el temor de evidenciar fallos de seguridad en los sistemas de información.

Esta situación ha generado que se considere que las acciones perpetradas en conexión con los medios informáticos son los casos de más índice de cifras negras en las estadísticas de eficacia policial y judicial.

Según J. Carroll "los delitos informáticos constituyen probablemente el ejemplo más importante de encubrimiento de la realidad desde Watergate" y al referirse al respecto apunta "es difícil determinar de forma exacta y fiable la magnitud de las pérdidas y el número real de delitos penales.

En un Coloquio sobre delitos informáticos y otros delitos contra tecnología informática, convocado y realizado en Wuzburgo, Alemania, en octubre de 1992, la Asociación de Internacional de Derecho Penal presentó un informe sobre los delitos informáticos basado en informes de sus países miembros, según el cual solamente el 5% de los delitos informáticos eran denunciados a las autoridades encargadas de hacer cumplir la ley, por eso sobre este particular me referiré a continuación.

## IV. CAUSAS QUE GENERAN LAS CIFRAS NEGRAS.

Varias son las causas por la cual se generan estas cifras negras. Una de ellas es la ausencia de medios adecuados para la detección y control de los hechos; pues como se conoce no siempre se cuenta con un sistema de seguridad en las entidades afectadas.

Por otra parte, la víctima desconoce el hecho la mayoría de las veces o, aún conociéndolo y sospechando fundamentalmente quién lo cometió, tiene dificultades para probar ambas cosas, tanto la perpetración del hecho como la figura del autor.

Descubrir el hecho no resulta fácil, las propias características del mismo lo impiden: por los medios que emplean las que son sólo conocidos por especialistas; por la facilidad del autor de borrar las huellas; por el tiempo que puede mediar entre las manifestaciones de la acción y la manifestación de los efectos, condiciones que afectan además a la realización de las pruebas para la substanciación del proceso.

En otras muchas ocasiones, la víctima no denuncia los hechos, pues teme reconocer que ha sido sujeto de uno o varios de estos comportamientos; o lo que es peor, evidenciar la ausencia o ineficacia de sus medidas de seguridad; también en muchos casos la víctima desconfía la efectividad del proceso jurisdiccional para enfrentar el caso; bien sea por la falta de mecanismos adecuados o por la ausencia de una legislación que contemple las acciones y determine las medidas a imponer.

De manera que las acciones generadas por el uso indebido de la Informática y la Comunicación pueden estar relacionada a figuras convencionales tales como el hurto, robo, fraude, estafa, espionaje, pero que al realizarse con auxilio de medios informáticos exigen de un reanálisis de los elementos típicos a través de los cuales se pueden subsumir estas acciones con las figuras delictivas vigentes.

Por otra parte, es importante resaltar también que estas acciones generadas por el uso indebido de las modernas tecnologías pueden tener rasgos totalmente nuevos y que no encuentran cabida en figuras convencionales cual puede ser por sólo citar dos ejemplos:

El productor y distribuidor de programas de efectos nocivos (virus informáticos, bombas lógicas, gusanos, entras manifestaciones);

el intruso en las redes; pero, sólo apuntamos la idea ya que sobre el tema volveremos en lo adelante.

Recurrimos nuevamente al Manual de la OCDE para resumir todo que hemos querido resaltar hasta este momento y que constituye el planteamiento problemático del tema para adentrarnos en consideraciones más particulares.

E1 Manual expresa lo siguiente: "(...) esta proliferación y ampliación de las tecnologías informáticas ofrece un aspecto negativo: ha abierto la puerta a conductas antisociales que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley, y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales. La sociedad sufre las consecuencias económicas de los delitos relacionados con el uso de computadoras, pero la verdad es que recurren a sistemas computarizados para prácticamente todas las actividades de la vida: desde el control de la circulación de autobuses, trenes y aviones, hasta la coordinación de los servicios médicos o la seguridad nacional. El más pequeño desliz en el funcionamiento de esos sistemas puede representar un peligro para la vida humana. La rápida expansión transnacional de las redes de computadoras en gran escala y la utilización de líneas telefónicas corrientes aumentan la vulnerabilidad de esos sistemas y las posibilidades de uso indebido o de actos delictivos. Las consecuencias del delito informático pueden suponer importantes costos económicos y un elevado precio en términos de seguridad humana."

## V. CONSIDERACIONES SOBRE LAS EXPERIENCIAS LEGISLATIVAS EN EL ÁMBITO INTERNACIONAL.

Ante la aparición de estas acciones en los países que se ha legislado sobre la materia, se han puesto en práctica dos vías de solución legislativa:

a) dedican un título a los llamados delitos informáticos.-

Agregar las figuras que se puedan generar por estas acciones a continuación de los delitos convencionales que puedan tener relación, o la inclusión de dichas acciones como figuras agravadas, según sea el caso.

Estas técnicas tienen partidarios y detractores, en lo particular estimo que es saludable hacer la revisión de los delitos convencionales y en lo posible atemperar su formulación a las nuevas condiciones de posibilidad de materialización de la acción por medios informáticos, pero en ningún caso debe apuntar a la adjetivación de "informáticos" de tales acciones porque en realidad lo que puede cambiar es el medio de comisión en algunos casos, en otros de lo que se trata es de delimitar el alcance y naturaleza del bien protegido.

Por otra parte, la consideración como delito informático es portadora de una lista prácticamente infinita -en virtud de las posibilidades que brinda la técnica- de acciones que pueden constituir delitos, cuya práctica ha demostrado en la casi generalidad de los casos, la insuficiencia de su aplicación a hechos concretos, por razones múltiples que van desde la pronta obsolescencia de la descripción de la acción hasta la falta de medios de prueba para demostrar el hecho.

En otra dirección, pienso que en realidad ante la existencia y dependencia de los sistemas informáticos, tal como apuntamos anteriormente, el bien jurídico a tutelar es la "Seguridad Informática", toda vez que es el sistema de normas de todo tipo adoptadas en los diferentes entornos informáticos para garantizar la integridad, disponibilidad y confidencialidad de los datos contenidos en dichos sistemas, por lo tanto las acciones atentan indiscutiblemente contra estos tres elementos consustanciales al tratamiento de la información y al desarrollo de los sistemas de tratamiento y comunicación de ésta.

Dichos elementos son tangibles y se pueden establecer con normas sustantivas que al ser violados -por culpa o negligencia- constituirían delitos.

En otro orden de cosas, es sabido también que existe una tendencia a regular los llamados "delitos informáticos" y los llamados derechos inmateriales en general, por legislaciones especiales, que en un mismo cuerpo legal especial se establezcan las normas sustantivas y las normas sancionadoras -medidas administrativas o penales- aplicables ante incumplimiento.

Generalmente, éstas modalidades han sido el fruto de primeras intentos legislativos en materia de Informática, que abarcan, además, áreas muy particulares de aplicación -uso de ficheros automatizados, protección de datos

personales, medios audiovisuales- que son legislaciones nacidas ya a finales de la década de los 60 en los principales países desarrollados, obviamente.

Toda esta experiencia legislativa ha ido llegando como práctica al resto de los países, y nos permite evaluar los resultados en la aplicación y eficacia de las mismas.

Entre las figuras más nítidas y realmente nuevas nacidas en la interacción hombre-máquina se encuentran las siguientes:

- El creador de virus informáticos o programas informáticos destinados a realizar acciones con fines de lucro;

- El distribuidor de virus informáticos o de informaciones sobre la elaboración de programas con fines "malignos".

- El "intruso" -acceso no autorizado- en las redes de información electrónica y en los sistemas informáticos.

Hay otras figuras que se generan en cierta forma de éstas, como la distribución y venta no autorizada de información electrónica.

Además, la consideración de este tipo de delito exige la delimitación de qué información es susceptible de estas normas, pues hay que recordar que la información es un recurso estratégico.

Este tipo de acciones tiene un punto de contacto con la protección de los datos personales, cuyos principios han sido reconocidos por Naciones Unidas.

En el "Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos" se dedica el Título II a la exposición de las leyes penales sustantivas que protegen a los poseedores de datos y de información.

Haciendo un muy breve recorrido por los antecedentes del tema de la Protección de Datos y las experiencias nacionales en la elaboración de los estatutos jurídicos que conforman el régimen legal vigente en esos países.

Para concluir con el tema de las conductas típicas en esta mirada internacional, podemos decir además, que un estudio comparativo de la

experiencia legislativa evidencia que las sanciones ante tales conductas abarcan tanto la multa administrativa, para casos no previstos en la legislación penal pero sí en legislaciones especiales, y el binomio alternativo o no de multa y privación de libertad, en caso de legislaciones penales.

En cuanto a la sanción también hay criterios divergentes, pues algunos estudiosos insisten en que debe ser una sanción penal, por el principio de proporcionalidad de las penas, pues son cuantiosos los daños que pueden ocasionar, lo que supera el marco impositivo por la vía administrativa. Además del valor ejemplarizante de la sanción penal.

En cuanto al tema apelo más al desarrollo de las tendencias de política penal al amparo del desarrollo del Derecho Penal y de las propias condiciones y tradiciones jurídicas de cada país.

## VI. LA SEGURIDAD INFORMÁTICA COMO OBJETO DE TUTELA JURÍDICA. UNA PROPUESTA PARA LA MODIFICACIÓN DEL ACTUAL CÓDIGO PENAL CUBANO.

El desarrollo creciente de las aplicaciones de la Informática en Cuba ha incrementado su dependencia a los sistemas automatizados.

Estos sistemas se pueden ver amenazados por diferentes acciones que pueden poner en peligro actividades tan importantes como la salud (fundamentalmente en relación con el diagnóstico clínico), las investigaciones científicas, los controles económicos y financieros, la automatización industrial, los servicios de reserva de pasajes, hoteles y otras capacidades, el pago de la seguridad social, el cobro de servicios como el telefónico, la electricidad, el gas, entre otros, todos los cuales al ser afectados causarían cuantiosos daños económicos y sociales.

Los actos nocivos generados por medios informáticos o contra estos en Cuba, al parecer no encuentran por parte del Derecho una respuesta enérgica pues obviamente se trata de nuevas conductas que se han generado o incrementado con posterioridad a las principales modificaciones de la legislación penal vigente. Pero la realidad es que existe un conjunto de tipos delictivos vigentes que resultan suficientes para enfrentar una diversidad de conductas indebidas, no obstante pensamos que como toda obra humana, nuestro Código es perfectible y que ante los desafíos tecnológicos generados por un sostenido desarrollo informático en un

país es necesario emprender estudios multidisciplinarios para su estudio y cuando proceda introducir las modificaciones que resulten necesarias.

Por ello, en la actualidad constituye un imperativo buscar una respuesta a tales acciones pues esa impunidad puede constituir un elemento que propicie la manifestación continua de tales aciones, de hecho en los últimos tiempos se nota un incremento en la incidencia de hechos.

Estas afirmaciones se basan en la experiencia de la Comisión Nacional de Protección de Datos, creada desde 1988, la cual desde entonces comenzó a estudiar el problema y a sugerir la implementación de un sistema integral de Protección de la Información.

Dicho sistema de protección está sustentado en el establecimiento de un régimen de Disciplina Informática que comprende todas las normas de uso y conservación de los sistemas automatizados y los datos en ellos contenidos, esto se realiza sobre la base del establecimiento del registro nacional de cada virus que existe o entra en el país, un sistema de alerta a todas las entidades y la realización de una versión en software de protección contra cada agente infeccioso, así como el establecimiento de medidas de protección entre las cuales se encuentra las modificaciones realizadas al Reglamento de Ferias y Exposiciones, en el sentido de disponer el control de protección de la información a todo expositor tanto nacional como extranjero, en evitación de la propagación de virus informáticos por el intercambio de información en soportes infectados y la propagación de nuevos de nuevos virus ya que éstos son detectados a su entrada al país.

Las cifras demuestran la efectividad de estas medidas. No hay que olvidar que según datos oficiales del Virus Test Center (VTC) de la Universidad de Hamburgo, aparecen diez nuevos virus informáticos como promedio diario en el mundo.

En Cuba donde hay alrededor de 80.000 computadoras que se utilizan en todos los sectores de la economía, han sido, detectados y aislados 141 virus, de un total de más de 10.000 virus existentes en el ámbito mundial. De esos 141 virus se han podido determinar que 14 de ellos son autóctonos o hechos para surtir efectos en Cuba.

De esos 141 detectados, no todos han llegado a propagarse por la eficacia en las medidas de protección.

También se ha trabajado en la formación de una cultura de utilización de las técnicas informáticas y en la formación de nuevos valores éticos.

Otras normas han sido recogidas en textos de limitado rango jurídico, como fue en su momento la Resolución N° 3 "Reglamento de Protección de Datos y Programas de Computación" promulgada por el INSAC, que ya no es un organismo de la Administración Central del Estado y cuyas funciones han pasado al Ministerio de la Industria Sideromecánica y la Electrónica. En tanto otras normas han sido establecidas por el Ministerio del Interior a través de Instrucciones.

En cuanto a este último Ministerio cabe señalar que en un esfuerzo sostenido por actualizar y atemperar la legislación vigente en materia de protección de la información, no sólo ha elaborado algunas normas de inferior rango jurídico, como resoluciones, sino recientemente aprobó un Reglamento que regula lo concerniente a la Seguridad Informática, lo que permite el análisis planteado, como objeto de tutela jurídica.

De igual forma en 1995 a través de un Decreto de Contravenciones se establecieron las primeras medidas administrativas, que sancionan conductas contrarias a la protección de la información que se procesa por medios informáticos.

Pero todo el esfuerzo que hasta hoy se ha realizado, no sería todo lo eficaz que queremos y necesitamos si no se complementa con otras acciones de orden práctico, como es la preparación del personal de instrucción policial y judicial.

No puede entenderse que contamos con un universo jurídico general, coherente, sistémico y sistematizador de las reglas de conductas en materia de Informática y comunicaciones electrónicas, pero estamos trabajando por ello.

Algunas disposiciones abarcan sólo una parte del problema, el virus informático, preferiría que fuera a los programas dañinos en general.

## VII. PRESENTACION DEL SOFTWARE ROGER.

Existen varios tipos de software diseñados especialmente para modificar o destruir sistemas de computación o datos informatizados.

A estos tipos de programas se les conoce dentro del medio como Software Roger[15], y dentro de ésta denominación genérica se agrupan cuatro tipos de programas: el Caballo de Troya, el Gusano, la Bomba de Tiempo, el Virus Informático.

A estos tipos de programas se le llaman genéricamente y erróneamente: "Virus Informáticos".

Sin embargo, es preciso destacar que existen substanciales diferencias entre cada uno de ellos en virtud de las técnicas de elaboración, los objetivos que persiguen y la forma de manifestarse, por eso no es correcto la consideración de que todos son Virus Informáticos.

VII. (a) - El Caballo de Troya

Un Caballo de Troya es un programa legítimo que contiene una sección de "código oculto", y a primera vista, parece un programa inofensivo, identificado generalmente con un nombre provocativo, que en pleno siglo XX "reproduce" el pasaje mítico del Caballo de la Iliada.

Este programa puede permanecer inactivo por un largo período de tiempo antes de activarse. Otro rasgo importante es que al carecer del efecto de autorréplica; su código pernicioso se activa una sola vez.

Este tipo de programa se utiliza para extorsionar funciones rutinarias provocando que el programa realice tareas no autorizadas, tales como la habilitación de cuentas bancarias a nombre de alguien violando todo el trámite de banco, incluso el depósito, o el otorgamiento indebido de un salario o beneficio de seguridad social.

■ [15] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

En los sistemas bancarios también se han introducido programas que contienen instrucciones que obligan al sistema a realizar operaciones de redondeo de cifras en los procesos de actualización de cuentas bancarias y depositar dichos resultados en una cuenta habilitada, proceso que se repite automáticamente infinidad de veces, sin ulterior intervención del autor; este método automático de fraude es comúnmente conocido como "técnica de salami".

Otro empleo malicioso que se le ha dado a este tipo de programas es para atacar los sistemas de empresas, introduciendo por vía legítima los programas en determinado entorno informático.

El "software lock" es un tipo de Caballo de Troya, que funciona como un dispositivo capaz de trabar un programa una vez que sea activado. También se manifiestan como un "crash programs".

VII. (b) - La Bomba de tiempo o lógica

La Bomba de Tiempo, conocida también como Bomba Lógica, es un conjunto de instrucciones que se autoejecutan en un momento determinado, dada determinadas condiciones, como puede ser la coincidencia de determinada fecha o la secuencia de algunas teclas.

Se reconoce como el método más común empleado para perpetrar sabotaje por medios informáticos, y se clasifica como un programa de actuación retardada, ya que su efecto puede ser el de destruir un programa o sistema computacional, o la introducción de una "rutina-cáncer" que distorsiona el funcionamiento del sistema del propio equipo.

VII. (c)- El Gusano

El Gusano, es un programa con identidad propia, que una vez que ha sido abierto, busca espacio libre en la memoria interna de la computadora y se autograba en dicha memoria hasta el desbordamiento físico de la misma.

Este tipo de algoritmo está orientado a que los segmentos de programas que se van generando mantengan comunicación con el segmento de programa por el que fueron creados, lo que indudablemente da el efecto de anillado de los

gusanos naturales. Su acción se manifiesta generalmente en la lentitud de ejecución del sistema.

El gusano está diseñado para atacar fundamentalmente sistemas de comunicación. Los programas que se autotransmiten o exigen de la acción del usuario para transmitirse a diferentes direcciones electrónicas.

Por ello su presencia es típica en los sistemas de redes, particularmente proclive en entornos de redes públicas de comunicaciones y en redes locales, donde se reproduce en cada una de las terminales, hasta que la cantidad de memoria que ocupa es tal, que ocasiona la caída o fallo del mismo.

El medio de propagación de estos programas lo constituye el correo electrónico, especialmente para atacar sistemas unidos en una misma red.

Por su capacidad de autotransmisión entendida en ocasiones como autorreproducción puede considerarse un antecedente técnico de los virus informáticos, más su diferencia fundamental es el carácter de identidad propia con respecto al virus informático.

VII. (d) - El Virus Informático

La utilización de las técnicas de elaboración típica del Caballo de Troya -código oculto-, de la Bomba de tiempo -activación bajo determinadas condiciones- o del Gusano -autotransmisión-, en la elaboración del Virus, es lo que ha originado en cierta forma el criterio de identificación de que todos estos programas son Virus Informáticos, pero tal como hemos expuesto no lo son, entonces ¿qué es un Virus Informático?.

El Virus Informático es un segmento de programa de computación con capacidad para autorreproducirse y que al ser ejecutado cambia la estructura del software del sistema y destruye o altera programas o datos, o provoca otras acciones nocivas, sin autorización ni conocimiento del operador[16].

■ [16] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

Su capacidad de autorreprodución, como técnica de programación, es lo que nos permite reconocer su analogía con los virus biológicos.

La elaboración y distribución de virus informáticos, es una de las diversas conductas disválidas que se manifiestan en la actualidad en grados realmente alarmantes. A sus antecedentes, características y tratamiento como acciones constitutivas de Responsabilidad me referiré en los tópicos siguientes.

## VIII. OTRA CONSECUENCIA DEL SOFTWARE ROGER

La analogía entre virus informáticos y virus biológico ha traído como consecuencia la asimilación por la Informática de otros términos tales como "profilaxis, vacuna, epidemia, infección, contagio, tiempo de incubación, antídoto, cuarentena", los que si bien no tienen en el medio una interpretación literal, sí su dominio y alcance en el lenguaje natural favorecen la interpretación y explicación de los nuevos fenómenos y la asimilación análoga también de determinadas prácticas las que por supuesto son ajustadas al entorno informático.

El chequeo de todo software nuevo y su registro en el control de la entidad es un ejemplo de medidas profilácticas y una acción muy importante en caso de que el virus necesite un tiempo de incubación para provocar su efecto.

Para comprender mejor todas estas manifestaciones es preciso conocer todo en cuanto al surgimiento y devenir en el tiempo de los virus; pero, la historia y evolución de los Virus Informáticos ha sido muy bien desarrollada por algunos autores cubanos, entre ellos el Ing. Edgar Guadis autor de una enciclopedia electrónica sobre el tema, por lo que sólo motivo a los interesados a que vayan a las fuentes originales[17] para que puedan conocer más sobre el tema, sólo me concentraré en los elementos que tipifican a los virus y a algunos argumentos jurídicos esgrimidos en su defensa desde su surgimiento.

La historia de los virus informáticos se remonta a los años cincuenta. Los primeros programas con fines de destrucción o alteración de información, fueron diseñados como medios de protección de Software con el ánimo de impedir su reproducción o ejecución no autorizada.

■[17]

Así quien intentase reproducir esos programas, se llevaría también, sin saberlo, unas instrucciones dentro del programa que copie, que no sólo impediría la ejecución del software pirateado, sino que destruiría toda la información de la computadora utilizada para el efecto.

De modo que podemos decir que los primeros virus, tuvieron origen protector, pero constituían una práctica de justicia por mano propia, donde se manifestaba una sed de venganza, más que lograr la equidad y resarcirse de los perjuicios ocasionados por el acto de piratería informática.

No es posible reconocer al virus como medio de protección, aunque sí reconozco el fin legítimo de protegerse, pero la propia informática brinda otros medios, uno de ellos puede ser la criptología -reconocido procedimiento que garantiza la confidencialidad y la autenticidad de la información-, a los que no se les puede imputar ineficacia porque los virus no han impedido tampoco los actos de piratería.

No es válido argumentar legítima defensa en un acto de premeditación como es la creación de un virus. Otro principio es válido, no puede causarse un mal mayor para defenderse de un daño, pues queda patente que el autor de un virus no se detiene a evaluar el perjuicio que su programa puede acarrear.

También fueron diseñados programas similares a los que hoy tipificamos como virus, para sabotear la ejecución de un programa, muchas de estas acciones de sabotaje perseguían un fin lucrativo o eran acciones en el que el autor pretendía reparar un daño, a veces en el plano laboral, que la entidad le había ocasionado.

En la actualidad ya no se puede decir que los móviles son puramente de protección, aunque reitero, protegerse empleando como medio un virus es totalmente ilegítimo.

Para la mejor comprensión de las implicaciones generada por la acción de los virus informáticos, es preciso descomponer la misma a partir de relacionar las características esenciales de estos programas.

VIII. (a) - Características de los virus informáticos

Del concepto de virus informático podemos extraer los elementos típicos que permiten determinar que estamos en presencia de un Virus. Estos son:

1. Es un segmento de código ejecutable: Esta característica implica que el conjunto de instrucciones que contiene el "programa" está orientada a que sólo bajo determinadas condiciones -la coincidencia de frases, nombres, fechas, lugares- se activen sus efectos.

Por ejemplo, el virus "Martes 13", se ejecuta al encenderse una máquina en la que la fecha calendario del equipo coincida con esa fecha. Por su parte la acción del virus 1530, se materializa al teclearse la 1530 a vez, otros como el virus Stoned anuncian su presencia al momento de la infección, pero ocasionan el daño al azar.

2. Producen un daño: Estos programas han sido diseñados para ocasionar un daño, cuyos efectos pueden determinarse inmediatamente, a corto plazo o largo plazo.

Los daños pueden ocasionarse tanto al hardware como al software. En cuanto a la información, la misma puede ser destruida total o parcialmente y también puede ser alterada, lo cual puede ser aún más peligroso, especialmente en sistemas de información diseñados para el auxilio en la toma de decisiones, como por ejemplo los diagnósticos médicos.

Con el correr del tiempo estos programas han aumentado sorpresivamente su capacidad destructiva.

Desde el punto de vista económico el daño que se produce con este tipo de acciones cuando se dirigen a bienes patrimoniales resulta de alto valor económico. Este daño puede derivarse de una o varias acciones, también pueden tener carácter continuado, o se manifiestan en infinidad de operaciones por un importe mínimo, modus operandi típico cuando se emplean técnicas de salami.

La lesividad de estas acciones se acentúa en la actualidad debido a la interconexión entre las actividades económicas, viéndose afectados varios receptores informáticos, por lo que el perjuicio aumenta considerablemente, esto es lo que se conoce como efecto de cascada, lo que además dificulta mucho la cuantificación del perjuicio.

La concurrencia en el delito de daños se determina por la producción efectiva de la destrucción o inutilización, admitiéndose las formas imperfectas de ejecución. Quizás el ejemplo más común sea determinar si la introducción de una rutina destructiva en el programa constituye un acto ejecutivo punible -tentativa- o uno preparatorio impune.

3.- Tienen la capacidad de autorreproducción: La reproducción parte de la existencia de un código "padre" encargado de iniciar la epidemia vírica.

Los segmentos de virus son capaces de reproducirse infinidad de veces en soportes magnéticos, al generar copias de sí mismos de forma homogénea o en parte discreta, en un fichero, disco o unidad física distinta a la que ocupa.

Esta condición conlleva a la multiplicación del virus con pocos o ningún esfuerzo y sin disponer el autor apenas de recursos, basta que el virus sea creado e introducido en determinado entorno para que pueda ser propagado, sin limitaciones de tiempo y espacio, incluso trasladarse de un país a otro, pudiendo establecerse cadenas mundiales de propagación de los virus informáticos.

Ello se debe a que el virus informático una vez que está en una computadora puede tomar el control temporal del sistema operativo o en ocasiones en los programas ejecutables, a los que infectan y convierte en un canal transmisor, por ende al ser ejecutado, trasmite el virus.

En estos casos cada vez que entra en contacto con un software no infectado, se autorreproduce en el mismo, de ahí que todo ambiente promiscuo de intercambio de disquetes y programas sea un entorno favorable para la fácil diseminación del software infeccioso.

Es importante resaltar además que por las mismas características de autorreproducción y objetivos para los que fueron creados, siempre que se den las condiciones mínimas necesarias, el daño que pueden ocasionar irremediablemente lo causará y de eso están conscientes sus autores.

Al igual que el efecto de daño se ha ido sofisticando, la capacidad reproductiva adquiere nuevas modalidades de presentación.

4.- No tiene identidad propia: Los virus informáticos al carecer de identidad propia, es decir, al no ser programas sino segmentos de código, tienen

una ejecución parasitaria para lo cual requieren endosarse en los programas ejecutables, a los que añade la tarea adicional la ejecución del propio virus.

Por tal condición el propio usuario -víctima de la acción- involuntariamente provoca la activación del virus al ejecutar el programa que lo contiene; que son generalmente los de uso más frecuente: procesadores de texto u hojas de cálculo y especialmente los propios programas ejecutables del sistema operativo, que son los que más se utilizan por los creadores de virus dada su estandarización en el mundo informático.

Así atendiendo a las partes que modifican los virus en su ataque éstos se clasifican en: Virus del sector de arranque y Virus de Programas.[18]

Hoy en día tienen gran presencia los Virus Macro que han introducido modificaciones en las concepciones de clasificación, por lo que resulta más conveniente hablar de virus que atacan al sector de arranque y virus de ficheros, entendiendo así que un fichero puede ser un programa ejecutable o un documento.

5.- Se manifiestan a través de diferentes acciones: Por la diversidad de manifestaciones, sólo limitada por la creatividad de sus autores, no se puede hablar de un "síntoma o patología" de los virus.

El abanico de manifestaciones abarca tanto desde el simple mensaje en pantalla para saludar o dar a conocer la presencia del virus en su máquina, así como la disminución de la velocidad de ejecución de las operaciones en su computadora.

Esta característica ha servido de base para la clasificación de los virus en benignos: el simple mensaje o en malignos: cuando hay afectación al sistema o los datos.

Tal clasificación es inaceptable, ya que toda acción de los virus afecta el proceso de tratamiento de información, lo menos que hace es interrumpirlo y ese tiempo es irrecuperable y tiene un costo.

■ [18] Notas del Curso "Derecho e Informática", Universidad de Zaragoza, 1991.

En síntesis el efecto maligno de los virus está dado en:

- comparte tiempo de ejecución;

- comparte memoria; y,

- comparte espacio en el disco.

6.- Son códigos residentes: Al carecer de identidad propia, es decir no ser un programa sino un segmento de código, los virus necesitan alojarse en la memoria de la máquina, para poder obtener el control permanente de funciones del sistema operativo.

7.- Su funcionamiento comprende dos fases definidas: Una primera fase es de infección o réplica. En analogía con los virus biológicos esta seria la etapa de incubación, pero esta etapa de "ocultamiento" es válida a su vez para la propagación, pues el código oculto se reproducirá todas las veces que sea posible.

La segunda fase es de ejecución, en virtud de la cual el código se activa al responder a la acción para la cual ha sido programado: la introducción de una cadena especial de caracteres, una fecha determinada o un tope de autocopias del virus alojado, la fase de ejecución se materializa en la consecución de efecto nocivo del virus.

Es importante resaltar que la acción de infección es inmediata.

8.- No muestran el rostro: Los virus son diseñados para ser introducidos en los sistemas sin que se note su presencia, por eso sus creadores los enmascaran, algunos utilizan en este enmascaramiento técnicas propias de los otros programas Roger que enunciamos con anterioridad.

De las características de los virus se puede concluir, además, que en todo acto de creación de un virus existe premeditación; ningún código o segmento de programa con estas características puede ser creado al azar.

VIII. (b).- La distribución de los virus informáticos y programas dañinos en general.

Comentario aparte merece la distribución del virus, los programas dañinos en general. Esta puede realizarse de manera consciente o inconscientemente, y puede darse por medios tradicionales, o en soportes magnéticos, así como a través de las redes.

De manera consciente el autor del virus, o un tercero, puede dar inicio a una cadena de contagio, basada en las características de reproducción de los virus. Es obvio que para cumplir sus objetivos estos sujetos se valen de fisuras en los sistemas de seguridad o violan la disciplina informática.

En el supuesto anterior el medio informático es el canal de distribución.

Pero en otros supuestos la distribución se da mediante la difusión de la información sobre virus y resulta posible mediante la publicación del listado completo de virus.

En estos casos, amparado en una trasparencia informativa, y en el entendido de que a mayor información y más conocimiento sobre el hecho, el impacto social es menor; el efecto es de "rebote", pues lo cierto es que a partir de la publicación de las cadenas de virus han aparecido más versiones.

Al parecer muchos programadores que hasta el momento no habían prestado atención a estos programas y que por sí mismos serían incapaces de crear un código nocivo, por no conocer los mecanismos de manejo de hardware a bajo nivel, los han empezado a experimentar con las instrucciones destructivas que han sido divulgadas.

Los efectos son conocidos por todos, con la variación se puede introducir modificaciones en el modo de activación, dando por origen a nuevas versiones de la cepa vírica.

## IX - LA RESPONSABILIDAD LEGAL ANTE EL SOFTWARE ROGER.

En este particular hay más preguntas que respuestas. Me permito citar algunos interrogantes y formular otros propios, para que la comunidad intelectual me ayude a despejarlas, pues insisto: el tema merece de respuestas.

Para muchos autores el virus constituye una modalidad de sabotaje y estimo que puede ser entendido como tal, aunque por los efectos puede ser subsumido en el delito de Daño.

Si analizamos a la luz de todo lo que hemos apuntado sobre este asunto vemos que existe una desproporción entre el gran perjuicio que se puede causar y la "gravedad" o modalidad del ataque.

No obstante quedan espacios oscuros y mucho que definir y desentrañar de estas manifestaciones; por ejemplo: la extrema sencillez de los métodos, a la que se añade la posibilidad de que los resultados se adviertan tras un lapso más o menos largo, facilita la impunidad de los autores; a ello se une además, la dificultad de valorar el perjuicio, a lo que se suma, también, la enorme diferencia entre éste y el valor material de los objetos destruidos.

Por eso es tan importante instrumentar los registros de activos: medios e información para poder valorar el monto del daño y en consecuencia exigir responsabilidad.

Supongamos que una entidad ha sufrido pérdida por un virus. ¿Se puede recuperar de ésta pérdida? Probablemente no y más si no tenía previsto un buen plan de seguridad informática.

Es evidente que existe una responsabilidad legal, y por tal motivo es necesario definir, entre otras, las siguientes cuestiones:

a)¿A quién se debe demandar? Los autores de virus no publican su existencia.

b) ¿Es responsable quién opera el equipo informático?

c) ¿Dónde se originó el virus?

d) ¿Se trata de un proyecto de alguna clase que alguien usurpó o fue claramente diseñado para dañar información? ¿O se trata de una técnica de programación empleada y que por descuido se ha propagado y por ende tener consecuencias nocivas para otro entorno informático ajeno al que fue diseñado?.

e) ¿Cómo fue liberado el virus? Fue sólo liberado de un software pirata. Para ser infectado, el usuario tenía que tener el software pirata instalado en su computadora.

f) ¿Le otorgaría un tribunal un recurso a un sujeto agraviado a causa de que utilizó un software "pirata"?

g) ¿Cómo se introdujo el software en el sistema?

h) Suponiendo que el autor del virus pueda ser identificado y la premeditación probada. ¿Es posible cobrar indemnización por daños?

i) ¿Qué ley deberá ser aplicada al autor de virus introducido, cuyos efectos se producen en un país diferente al de su residencia?. ¿La de su país o la ley donde se produjo el daño?

j) ¿Es el autor del virus el único responsable del daño?

k)¿En qué sentido puede la ley condenar a un autor de un virus que nunca tomó ninguna participación activa en su distribución del programa?

l) En el caso de la Bomba Lógica, algunos estudiosos se han preguntado: ¿Cómo se determina el grado de ejecución de un acto ilícito consumado por la introducción de un programa del tipo "Bomba de Tiempo", cuando el sujeto introduce la orden o cuando ésta se ejecuta?

m)¿Cabe en este caso la posibilidad de comisión imprudente, o estamos siempre en caso de dolo?

## X. LOS SUJETOS ACTIVOS O DELINCUENCIA INFORMATICA.

Si bien coincido con otros autores que no se puede hablar de un tipo de delincuente único con características propias y definidas, pues al decir de Lafuente, "el panorama es amplio y variado, desde el ratero aficionado, al administrativo furtivo, pasando por el timador casual y el niñato adolescente y desocupado, hasta llegar al profesional astuto, que emplea medios sofisticados para alcanzar un lucrativo fin". Si hay algo común: el sujeto es un conocedor de la técnica, y sólo personas con conocimientos técnicos pueden ser autores del delito.

El término "delincuencia informática" ha sido acuñado como categoría exclusivamente criminológica y se ha empleado para aludir a las conductas disválidas o indebidas que tienen vinculación con las nuevas tecnologías de la información y la comunicación.

También se emplea la expresión para referirse a todos los actos, antijurídicos según la ley penal vigente, socialmente perjudiciales y penalizables en el futuro, realizados con empleo de un equipo automático de procesamiento de datos.

Unido al tema surgen las discusiones al intentar esclarecer a qué forma de criminalidad se hace referencia cuando se habla de "delincuencia informática".

Algunos estudiosos como Luis M. del Pont y Abraham Nadelsticher lo consideran como un delito de cuello blanco. Calificación que tiene partidarios y detractores; mientras otros la inscriben en la delincuencia económica o como un subgrupo de la de guante blanco.[19]

La delincuencia Informática no es subsumible en ninguno de los dos tipos de delincuencia aludida: de cuello blanco o delincuencia económica, sino que debe constituir una categoría criminológica aparte; y sirven de fundamento a esta afirmación investigaciones empíricas llevadas a cabo en Estados Unidos, en las que se constata que el autor sólo en ocasiones pertenece a altas capas de la sociedad. Otras investigaciones realizadas en España ponen en evidencia que los autores pueden ser primarios u ocasionales y que generalmente se trata de empleados de las empresas afectados.

Por su parte, los criminólogos han empezado a expresar las características y particularidades en las cualidades internas de los individuos actores de estas actitudes, a partir del estudio de los que han sido identificados como autores de delitos.

Al caracterizarlos señalan los rasgos de personas solitarias y poco comunicativas, lo que hace poco frecuente la coautoría con estos actos.

Otros rasgos que reconocen estar presentes en los autores es el resentimiento e insatisfacción familiar, personal o profesional y muchas veces hasta desadaptados sociales.

También se destaca el rasgo de que no hay disposición delictiva inicial, esta nace más bien de su contacto con el sistema informático.

Y aunque sin ser un criterio unánime muchos estiman que los autores de delitos informáticos son altamente calificados desde el punto de vista técnico, incluso por encima del promedio, lo que explica la perfección técnica y operacional de los delitos.

■ [19] Dr. Antonio Millé, "El Derecho de Autor y la Infraestructura Global de la Información en las Américas", Seminario sobre Derecho de Autor y Derechos Conexos para países de América Latina.

De modo que no se trata de un autor común, por lo que además de las circunstancias psicológicas y socioeconómicas que deben tomarse en cuenta en su estudio criminológico, deben sumarse una serie de variables particulares.

## XI . ENTONCES, ¿CÓMO SE PUEDE ENFRENTAR EL PROBLEMA?.

Está claro que la solución no es una sola, sino varias, incluso algunas no excluyentes entre sí, y son de muy diferentes características y alcance.

Están dados en el ámbito de la administración de las organizaciones, en el plano técnico informático, en el legislativo y muy especialmente en el ámbito de la Deontología.

Tal como adelanté existe una clasificación más o menos coincidente entre los especialistas sobre acciones generadas por el uso de medios informáticos, algunas ya tipificadas como delitos.

Como apunté en otra parte de este trabajo, el aspecto penal es sólo una parte del problema, se trata de dotar a la sociedad de las medidas efectivas para evitar y protegerse del efecto nocivo de tales conductas, incluso a convivir con ellas; y no de adjetivar de "informáticos" acciones delictivas constituidas en nuestros códigos, sino de evaluar las características fundamentales que revisten estas actitudes y de qué modo pueden tener una respuesta real.

Por eso es necesario además conocer similitudes y definiciones, para poder conseguir una protección jurídica eficaz sin caer en el casuísmo, ya que casuísmo provoca lagunas legales e inaplicabilidad.

Dicho de otro modo: desde el punto de vista legislativo somos partidarios de la fórmula de número apertus; aunque como hemos dicho, también hay que crear tipos especiales: producir programas dañinos; distribuir programas dañinos; el intruso. Por otra parte, estimamos conveniente considerar a la Seguridad Informática como un bien atacable y por ende tutelable jurídicamente, en el entendido de que por acción o por omisión se puede atentar contra la disponibilidad, integridad y accesibilidad de la información digitalizada o de los sistemas y redes.

Tal consideración está fundada en el propio carácter multisectorial del impacto social de las nuevas tecnologías, que obliga a la reconceptualización de muchos conceptos tradicionales: "cosa juzgada, correspondencia, documento jurídico, bienes"; y además, en la necesidad de búsqueda de respuestas integrales, en evitación de la hipertrofia en las ramas del Derecho. La acción penal debe concebirse bajo el principio de intervención mínima, pero intervención suficiente.

Para tratar con realismo jurídico y práctico el fenómeno, se requiere un análisis especial, en cuanto a sus formas de manifestación y medios de comisión de la acción; delimitar qué bienes atacan y qué valores ponen en peligro; y determinar en qué medida se pueden prevenir y reprochar suficientemente estas conductas.

Lo que presupone que hay que determinar el valor del bien jurídico tutelado, la intensidad del ataque y el contexto social en que se manifiestan.

Además, debe atenderse al beneficio que reporta el hecho para el comisor, el daño que provoca, tanto al entorno físico del sistema, o al hombre en sentido amplio -individuo o grupo- en su integridad física, honor o patrimonio; y se precisa delimitar en qué supuestos las nuevas técnicas de información son empleadas como instrumento o medio para realizar la acción, o como fin para alcanzar determinado objetivo.

Es imprescindible que previa a la conceptualización penal, exista una regulación administrativa en materia de Informática que sirva de marco jurídico y defina el ámbito de actividad Informática los supuestos y conductas válidas y las acciones reprochables, además de establecer un sistema legal de medidas de seguridad que funcione como eficaz control con finalidad preventiva.

Luego, se debe evaluar concienzudamente hasta qué punto los tipos penales tradicionales pueden ser reformulados y adecuados, en tanto figuras específicas o agravadas, de manera que sean suficientes para subsumir en ellos una conducta determinada.

Si del análisis anterior se llega a la conclusión que lo más conveniente es introducir en la legislación modificaciones que conlleven la adición de nuevas figuras, bien sea en legislaciones especiales o en el propio Código Penal, los legisladores deben tener presente que la Sociedad de la Información está en fase de transición progresiva, por lo que al legislar se debe evitar el casuísmo excesivo

-no se puede pretender recoger todos los supuestos- porque además, dichas tipificaciones pueden quedar en breve en desuso, debido al acelerado ritmo del desarrollo tecnológico y las posibilidades de constante surgimiento de nuevas formas de manifestación, condición que es válida también para la reformulación de tipos tradicionales.

Coincido con el Dr. Emilio del Peso, en el sentido de que si a la par de la formalización jurídica no se presentan estudios doctrinales profundos, no sólo no se resolverán las cuestiones para los que fueron creados tales postulados, sino que se contribuye al surgimiento de nuevos problemas, cuestiones éstas que están además muy vinculadas a la formación del personal que enfrentará este tipo de delitos.

Por otra parte, tal como expusimos con anterioridad estos fenómenos se manifiestan en muy diferente grado en el concierto de las naciones, por lo que asumir modelos normativos puede dar lugar a serios problemas de ineficacia legislativa.

## XII. UNA INTERROGANTE DEL "MAÑANA" QUE ES "HOY": ¿ES NECESRIO UNA LEGISLACION PARA EL CIBERESPACIO?.

Al decir del Dr. Vittorio Frosini "(...) Esta es la nueva forma de la información, asimila en nuestro tiempo de civilización tecnológica, después de las formas anteriores de información verbal o gestual, simbólica con dibujos y con escritura, y más tarde con la imprenta y con los medios de transmisión eléctrica, hasta llegar al actual tratamiento (...)"[20], en nuestro caso la información digital.

Unido a este devenir de desarrollo tecnológico, la humanidad ha ido identificando un cambio en los paradigmas en cuanto al soporte de las informaciones, pero ninguno ha sido tan trascendental como los que son fruto de la Revolución Informática, hito en el desarrollo social a partir de la cual se comienza a gestar lo que hoy se conoce indistintamente como "Sociedad de la Información" o "Sociedad del Conocimiento" e incluso algunos la identifican

■[20] Antonio Enrique Pérez-Luño, "Impacto social de la nuevas tecnologías" pág. 15 Editorial Fundesco, 1987.

como la "Era digital", en cualquiera de ellas encontramos que en el vértice de todas estas realizaciones y como piedra angular sobre la cual erigen a la información.

Al aproximarnos al fenómeno nos encontramos que una de las características de la Sociedad de la Información es la convergencia en los medios de transmisión de información: Sistemas Informáticos y Sistemas Telemáticos de múltiples tecnologías y soportes a través de los cuales se almacena, procesa y trasmiten diferentes tipos de información (texto, imagen y sonido) a partir de las cuáles se genera el mensaje.

Por lo tanto, se ha definido al mensaje hoy en día "como una información trasmitida en la cuarta dimensión, aquella de la cognocibilidad pura, similar a la de la memoria y el pensamiento humano, ya que la elaboración de los datos por obra del computador se produce a una velocidad que se mide en millonésimas de segundos, y su transmisión en tiempo real anula las distancias, el espacio y el tiempo (...)".[21]

Así el desarrollo de la infraestructura mundial de información está transformando ya nuestro entorno común, especialmente en lo que se refiere a la generación y transmisión de conocimiento, convirtiéndose a su vez en generador de nuevas fuentes y formas de realización de empleo, por ende trasciende a nuestra vida cotidiana.

En la actualidad la información ha adquirido características de bien social, económico y jurídico autónomo. En cuanto a su forma, se ha separado de su continente tradicional: el paradigma papel, que hoy convive con el soporte digital; sin embargo la información se ha independizado de los mismos sin perder su identidad y su función.

Por otra parte, a la información se le reconoce valor como materia prima fundamental en el cuarto sector industrial. Se identifica además, como un recurso estratégico para el desarrollo; de manera tal, que los cambios estructurales son

■[21] Se estima que las pérdidas de información, oscila anualmente entre los US$ 3 y 5 millones. Esto en una empresa grande; en una empresa pequeña, la pérdida de información puede significar el fin de su existencia.

palpables en términos de indicadores de crecimiento económico, ya se comienza a distinguir entre países inforricos e infopobres.

También se reconoce, que la aplicación de las nuevas tecnologías de la información y la comunicación al entorno social en general es fuente de un sector productivo en tanto genera bienes y servicios y modos diferentes de realización del comercio internacional.

En el ámbito social, surgen oportunidades sin precedentes para la comunicación lo cual favorece extraordinariamente procesos de generación e intercambio de información.

Entre los componentes que integran esta estructura global de la información identificamos al factor humano; a la información que como se dijo es el elemento estratégico y la infraestructura material: el equipamiento (incluidas las telecomunicaciones) y el software, que son los que constituyen los elementos indispensables a través de los cuales se materializa esta realidad.

Todo ello deriva en consideraciones ético-jurídicas sobre el tratamiento digitalizado, el uso y la conservación de la información; tanto a través de los sistemas ya tradicionales de información, como en las más modernas formas de acceso, distribución y comercialización de la información que existen actualmente: las redes digitales de servicios integrados (ISDN) y las redes de comunicación de datos de alta velocidad.

Ante estas realidades entonces nos hemos empezado a preguntar: ¿Es necesario una regulación jurídica para INTERNET?; por el momento, es igual que preguntarnos: ¿es necesario ordenar jurídicamente el ciberespacio?.

Desde hace algún tiempo algunos juristas y otros profesionales, así como usuarios en general, han hablado del tema, algunos niegan toda posibilidad, otros a los cuales me afilio pensamos que se puede y se debe emprender desde el Derecho, pero la viabilidad para el establecimiento de un marco regulatorio del Ciberespacio exige una mixtura entre el Derecho que conocemos y el del porvenir, que es el que ya estamos necesitando hoy.

En otras palabras; y qué mejor que las expresadas por el profesor Michel Vivant, en La Habana, en marzo de 1996.

( . . . ) "si las redes no son espacios de no-derecho, hay respuestas en el "arsenal" jurídico (...). Seguro no son perfectas y es la razón por la cual debemos revisar las soluciones conocidas para explorar pautas nuevas (...)"[22].

Entre las cuestiones que quiero resaltar para contribuir a la respuesta es la necesidad de abordar el problema desde la coordinación entre los países que conformamos el concierto de naciones, pues tal como se ha apuntado ya aquí en este foro, uno de los problemas fundamentales es la jurisdicción y la competencia.

No creo que sea difícil lograr la coordinación, máxime cuando este propio espacio de realización del Derecho es paradigmático en cuanto acelera los procesos de comunicación e intercambio de información de modo impresionante: entonces de lo que se trata es de asumir una voluntad de contribuir a la solución de problemas.

Por otra parte, si bien es cierto que se plantean cuestiones cada vez más complicadas para el Derecho Internacional pero a la vez se nos brinda la posibilidad de lograr una mejor realización de su papel en el sentido de desempeñar una función más activa, tanto como orden normativo así como a través de instituciones internacionales, lo cual pone en evidencia que se trata de cuestiones de hecho además del Derecho[23]. Por lo tanto, si bien pienso que las soluciones pueden ser logradas desde el Derecho no creo que exclusivamente desde éste.

En tal sentido, pienso que es necesario fomentar valores éticos, por eso atribuyo mucha importancia a los códigos deontológicos, lo que condiciona que para su efectiva autorregulación es necesario crear o reconocer espacios competentes, no obstante se sabe que no siempre las normas del deber ser son cumplidas, entonces interviene el Derecho para exigir responsabilidad.

■[22] Carlos Ferreyros, "Aspectos metodológicos del delito informático", Notas del curso Nuevas Tecnologías y Derecho, UNED, mayo de 1995. Mérida, España.

■[23] Antonio Enrique Pérez-Luño, "Impacto social de la nuevas tecnologías" pág. 15 Editorial Fundesco, 1987.

También considero que el fomento a asumir conductas éticas, resulta además una garantía de un cumplimiento consciente de las normas jurídicas, que es en definitiva a lo que se aspira en tanto eficacia social del orden legal.

En este sentido, entonces podemos hablar de un espacio habitable civilizadamente en el que se integre armónicamente: el factor humano, la información y la infraestructura material, que curiosamente como fruto de la creación intelectual como lo es el software también tiene que ser protegido.

El proyecto de las autopistas de la información quedaría en una aspiración sin ricos y abundantes contenidos, pero la existencia de los mismos dependen de la seguridad de sus propietarios de ser respetados en sus derechos.

Como se conoce, la vida en el espacio informático ya está generando prácticas, roles y valores diferentes. La relación jerárquica de los bienes también está cambiando. Por lo tanto el mundo jurídico debe reflejar esa realidad produciendo las normas que sean necesarias para impulsar el progreso y mantener un justo equilibrio de intereses en las partes que participan en este proceso. Aunque se debe propiciar la participación de todos en las oportunidades que brindan las nuevas tecnologías de la información y la comunicación.

En el ámbito del Derecho que protege las creaciones de formas, debe tomarse en cuenta el aumento de la importancia de los derechos de acceso, transmisión y usos de la información digitalizada, para reformar consiguientemente su protección legal. El alcance del derecho a la integridad deberá revisarse, para adaptarlo al actual estado del arte.

Debe atribuírsele importancia de primer rango a lo referente a la difusión de normas para la información sobre Propiedad Intelectual, así como de otros segmentos especializados del Derecho que confluyen en estas realidades, lo cual tiene implicaciones en cuanto a las reglas de publicación y divulgación del orden legal.

La información y la protección técnica a los archivos y medios digitales debiera recibir fuerte tutela jurídica, incluso por vía de la sanción penal, según corresponda, aunque en todo caso se debe propender al uso racional y permitir un tratamiento como recurso estratégico.

Coincido con el Dr. Antonio Millé, que en este proceso evolutivo del orden legal, "los cambios jurídicos deben preparase al detalle, la intensidad y la calma que los generosos plazos disponibles autorizan, no emprender tal proceso con urgencia implicaría la seguridad de frustrar parcialmente uno de los mejores esfuerzos de la humanidad tiene en el horizonte cercano."[24]

Es imprescindible atacar el problema desde el frente internacional. La ausencia de un mínimo uniforme de protección a lo largo del mundo crearía "desiertos de información" eludidos por el tráfico de contenidos, se arriesgaría la aparición de "paraísos de piraterías" desde donde se atribuyen contenidos usurpados o adulterados, al tiempo que se facilitaría aun más la circulación de programas dañinos, expresión de justicia por mano propia, en mi criterio un retroceso en el desarrollo de la humanidad; así como la proliferación de una nueva forma de cometer actos de agresión, los cuáles ponen en peligro infinidad de intereses: sociales, políticos, económicos e incluso la propia seguridad nacional y la soberanía.

Por otra parte, en cuanto a los aspectos técnicos (materiales técnicos) hay que continuar incorporándolos al servicio de la humanidad, en el sentido de utilizarlos como recursos materiales para garantizar la tranquilidad y el cumplimiento de ciertos presupuestos de Derecho.

El propio desarrollo tecnológico puede y de hecho lo hace, brindarnos muchas posibilidades de protección real y eficaz, asumiéndose por nuestra parte el rango de previsión posible del riesgo y de vulnerabilidad que ellas mismas son portadoras, por lo que es necesario diseñar e implementar políticas y estrategias de Seguridad Informática, reconocer el justo e imprescindible valor de los procesos de Auditoría Informática, al tiempo de dedicarnos a fomentar una cultura de protección de la información.

Para ello se exige invertir en recursos y esfuerzos en la formación del profesional del Derecho, en el sentido de contar con operadores jurídicos capaces de enfrentar este reto tanto culturalmente como en un ejercicio eficiente de sus

■[24] Se estima que las pérdidas de información, oscila anualmente entre los US$ 3 y 5 millones. Esto en una empresa grande; en una empresa pequeña, la pérdida de información puede significar el fin de su existencia.

funciones y desempeños profesionales. Lo mismo sucede con el profesional de instrucción policial para poder contar con cuerpos especializados en prevenir y perseguir los actos indebidos que pueden ser cometidos.

Sin embargo, pienso también que este esfuerzo sería menguado si se alcanza al ciudadano común, usuario potencial de toda esta la tecnología.

Comencé citando al profesor Vivant, inspirador de estas meditaciones y termino también con una reflexión que me sugiriera: pensemos en un Derecho no para el mundo virtual sino para los hombres que asistimos a él.

Al decir de José Martí. "Para qué sino para poner paz entre los hombres han de ser los adelantos de las ciencias".

## XI - BIBLIOGRAFIA


- Amoroso Fernández, Yarina - "La Informática como objeto de Derecho", Revista Cubana de Derecho No. 1, 1990.

- Correa y otros,- "Derecho Informático", Ediciones Despalma, Buenos Aires, 1987.

- B. Parker - "Combatte la criminalité informatique". París, Editorial Oros, 1985.

- del Pont, Luis y Nadelsticher - "Delitos de Cuello Blanco." Cuaderno No.8 del Instituto Nacional de Ciencias Penales (INACIPE), México, 1981.

- Facultad de Derecho - Actas del Congreso sobre Derecho Universidad de Zaragoza Informático, 1990.

- Ferreyra Cortes Conzalo - "Virus en las computadoras", 2a Edición. Macrobit.tm, México 1991.

- Ferreyros, Carlos - "Aspectos metodológicos del delito informático", Ponencia II Congreso Internacional de Derecho e Informática.

- Lima, María de la Luz -"Delitos Electrónicos" Trabajo presentado para ingresar a la Academia Mexicana de Ciencias Penales.

- Pérez-Luño, Antonio E. - "Impacto social de la nuevas tecnologías", Editorial Fundesco, 1987.

- Téllez Valdés, Julio - "Derecho Informático",. Editorial Instituto de Investigaciones Jurídicas, Serie A: Fuentes, b) texto y estudios legislativos, No. 75.

Citas:

- Vittorio Frosini, "Humanismo y Tecnología en la jurisprudencia". Revista internagionalle di filosofía del diritto, 1965.

- Vittorio Frosini, "Hacia un Derecho de la Información", Ponencia presentada en el II Congreso Internacional de Derecho e Informática, Mérida, España, 1996.

- Vittorio Frosini, Obis, Cit.

- Chaumoux, "L' appropation de l' information", Libraries Tecniques, París, 1986.

- Chaumoux, Obis. Cit.

- Yarina Amoroso Fernández, "Informática en Clave Jurídica. Apuntes para un estudio del orden legal cubano. Premio Ensayo en el Concurso de la Sociedad Cubana de Derecho e Informática, UNJC 1997.

- Carlos Lage, Informe económico al V Congreso del Partido Comunista de Cuba, 1997.

- Documento "Programa de Informatización hasta el año 200", elaborado por un grupo de especialistas de los OACE: SIME, CITMA, MICOM y MINJUS, 1997.

Bibliografía:

- Tecnología de la información, su impacto social y su consecuencia legislativa. Algunas consideraciones. UNESCO.

- Conferencia General. 29° reunión, 29 c, Punto ó.4.

- Vittorio Frosini: "Hacia un derecho de la información", Revista Informática y Derecho, No. 12, 13. 14 y 15 - Actas del III Congreso Internacional de Informática y Derecho, Mérida, UNED, España, 1996.

- Pierre Catalá: "Ebanche dúne theorie juridique de l'information, Reeveil Dalloz, 16° cahier, Cronique, 1984.

- Antonio-Enrique Pérez Luño: "Nuevas Tecnologías, Sociedad y Derecho. El impacto sociojurídico de la N. T. de la información. Libro Fundesco, 1987.

- Horacio H. Godoy: El reencuentro de la ética con la ciencia y la tecnología en las puertas del siglo XXI". Ponencia IV Congreso Iberoamericano de Derecho e Informática, Bariloche, Argentina 1994.

- Horacio H. Godoy: "El Espacio Informático". Ponencia IV Congreso Iberoamericano de Derecho e Informática, Bariloche, Argentina 1994.

- Antonio-Enrique Pérez Luño: "Los derechos de la era tecnológica en la obra de Vittorio Frosini". Revista THEORIA - segunda época No. 16-17-18 tomo B. 1992.

- Michel Vivant, "Lamy Droit de 1' Informatique",Ed. Lamy, S.A, 1997.