Contribución al debate sobre la conveniencia de una legislación en Internet

YARINA AMOROSO FERNÁNDEZ

Ministerio de Justicia de Cuba

A modo de introducción:

Hablar de los virus informáticos resulta un tema muy interesante por lo complejo que resulta, al tiempo que tiene gran actualidad; todos nosotros podemos en cualquier momento ser víctimas de un daño provocado por una acción de un virus.

Al parecer no existe conciencia muy clara de su trascendencia e incluso para algunos el tema pertenece más al mundo de la ciencia-ficción que a nuestra realidad cotidiana, para otros es una broma pesada. Para los autores intelectuales o materiales de estos programas dañinos existen diversas motivaciones y circunstancias materiales que le propician dedicarse a ello. Por eso el hecho de los virus no es sólo tecnológico, sino también social y por ende tiene repercusión en el ámbito de lo jurídico.

Tampoco puede verse al virus como un fenómeno aislado de manifestación de conducta indebida generada en la interacción hombre-máquina, pues hay varias manifestaciones de los llamados Delitos Informáticos que pueden ser generadas a través de la acción de programas de virus.

Por estas razones el trabajo que hoy presentamos a ustedes, se desarrolla a través de los tres puntos principales:

1. - Destacar las nuevas tecnologías de la información y la comunicación como fenómeno en sí, para desentrañar las causas objetivas en que se generan estas conductas.

2. Esbozar algunas conductas típicas de los llamados Delitos Informáticos, para acercarnos a las soluciones legislativas de algunos países y desentrañar ciertos elementos típicos presentes en las conductas contempladas en legislaciones penales y que tienen puntos de contacto con las manifestaciones de los virus informáticos.

3. Analizar a los virus informáticos en comparación con otros programas dañinos como el Caballo de Troya, la Bomba Lógica, el Gusano, entre otros, y evidenciar partiendo de la diserción del comportamiento de los virus los elementos que están presentes en los mismos que nos permiten hablar de aspectos legales de los virus informáticos.

A colación del tema se abordan algunos elementos sobre la delincuencia informática y el fenómeno de las cifras negras que generan estas conductas.

Con este trabajo pretendemos más motivar el debate que dar respuestas; las consideraciones que planteamos son el resultado de nuestra experiencia de investigación en el Laboratorio Latinoamericano contra Virus Informáticos (PII-UNESCO).

I- NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN: LA INFORMÁTICA COMO FENÓMENO EN SI

Con razón se ha afirmado que las Nuevas Tecnologías de la Información y la Comunicación son algo más que una moda; la Informática y la Telemática, expresiones más sintéticas de este fenómeno y devenidas en ciencias, son ya un elemento más de nuestra vida diaria.

Con respecto a la Informática, desde sus orígenes, en 1890, cuando Herman Holleriht inventa un sistema capaz de realizar tabulaciones, y decisivamente cuando en 1954 se comercializa por primera vez un microprocesador, el hombre se ha empeñado en ofrecer soluciones a los problemas de velocidad, volumen, capacidad y costo.

Así, gracias a los estudios y aplicaciones de silicio, ha logrado una velocidad de procesamiento más de 2.000 veces superior a los primeros ordenadores y reducir su costo en más 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 las nuevas Tecnologías de la Información y la Comunicación, y que se refleja en todo cuanto está asociado a las partes físicas de la computadora (hardware), y que alcanzó también a la parte inmaterial (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 él se han destinado fuertes inversiones con el objetivo de contribuir al desarrollo de aplicaciones y programas al servicio del hombre.

Producto de éste vertiginoso desarrollo, hoy contamos 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.

La Informática ha devenido un elemento estratégico en el sistema de organización y de producción de la sociedad, cuya principal vocación es aumentar la productividad.

En la actualidad se ha ampliado considerablemente los ámbitos de aplicación en la actividad humana y ha llegado alcanzar decisivamente las actividades jurídicas; pero a su vez; las nuevas tecnologías han sido y son materia de regulación por el Derecho.

La importancia de la Informática es necesario analizarla del lado de sus características específicas, así como de los profundos cambios que se vienen sucediendo en nuestro planeta en los últimos decenios.

Se atribuye a la Informática cuatro características que están en directa relación con el efecto multiplicador que ha producido en las actividades sociales; particularmente en el aumento de la productividad técnica.

La Informática posee una primera característica principal, pues permite mayor velocidad de cálculo que aquella realizada por el hombre.

Una segunda característica relacionada con la primera es la de asociación y relación lógica; y una tercera, que es la relativa memorización, es decir, al almacenamiento de datos, informaciones, imágenes y sonido.

Una cuarta característica es la relativa a la posibilidad de comunicación de estos datos, informaciones, imágenes y sonidos.

Esta última característica es la que puesto en franco cuestionamiento la eficacia protectora de los Derechos de Propiedad Intelectual, ante las nuevas formas de reproducción y creación artísticas, tales como la Multimedia y la páginas Web, y la circulación de obras intelectuales a través de redes de alcance global o local.

La doble relación entre la Informática y el Derecho se identifican metodológicamente, en dos disciplinas, cuyos objetos de investigación y de actividad son claramente diferenciados: Informática jurídica y Derecho de la Informática.

Por la primera entendemos todas aquellas actividades que la Informática elabora, aplica, procesa para incrementar la productividad en el ámbito jurídico y que debe contribuir a la realización de los principios fundamentales del Derecho.

La segunda relación abarca todo cuanto regula o intenta regular a las actividades relacionadas con la Informática en general y con las tecnologías relacionadas con ésta en particular.

Pero sería un planteamiento eminentemente normativista suponer que el Derecho de la Informática es sólo las normas jurídicas emergentes de estas relaciones, con lo cual sería limitarlo a una rama de la legislación que por demás existe.

El Derecho de la Informática, entiendo que abarca, además, el estudio, sistematización, contemporización de las nuevas relaciones sociales y jurídicas

emergentes de esta incidencia y su correspondencia armónica con un orden legal, social, económico e histórico, fruto del devenir de la sociedad. Esta sociedad que hoy vive y convive en dimensiones diferentes de espacio y tiempo.

La Telemática, por su parte, no es más que la conjunción de las enormes posibilidades de la Informática con el desarrollo vertiginoso de las técnicas y ciencias de las Telecomunicaciones para llegar a permitir que las barreras de tiempo y espacio se simplifiquen o desaparezcan y pongan en franco cuestionamiento la coexistencia de las fronteras territoriales internacionalmente reconocidas, ante la existencia real de un nuevo espacio de existencia y convivencia el Espacio Informático.[1]

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[2]. Estas últimas, permiten con facilidad desconcertante y apenas inimaginables, almacenar, recuperar y diseminar la información.

Pero la Informática y/o más ampliamente la Telemática[3] no es un fenómeno exclusivamente tecnológico, con implicaciones estrictamente positivas. Sus efectos dependen del uso que se les den.

De ahí que a finales del siglo XX, el balance del desarrollo de la Informática exhiba enormes posibilidades y aciertos, como efectos indeseables. Por eso intentaré hacer breve referencia a algunos de los efectos no queridos por todos con respecto a las Nuevas Tecnologías de Información y la Comunicación.

Por ejemplo, se ha hecho evidente en la última década el creciente interés del mundo en desarrollo en relación con las nuevas tecnologías de la información y comunicación; ello se debe a que la "Revolución Informática", introdujo transformaciones radicales en las relaciones de producción y la división

■[1] HORACIO GODOY, Horacio.: Intervención Especial en el IV Congreso Iberoamericano de Derecho e Informática, Bariloche, Argentina, 1994.

■[2] PEREZ LUÑO, Antonio Enrique: "Nuevas Tecnologías, Sociedad y Derecho", Editorial FUNDESCO, 1987.

■[3] Obis. Cita.

internacional del trabajo[4]; asumiendo las nuevas tecnologías un papel más relevante entre la llamada industria de los servicios.

Pero, es importante recordar que en la actualidad el diseño, producción y distribución de componentes electrónicos, equipos y software, están controlados por un muy reducido grupo de países desarrollados.

Esta centralización del poder sobre recursos cuya producción exige una compleja organización industrial, económica y educacional, limita la posibilidad de acción de los países que carecen de infraestructuras adecuadas y los pone en situación de desventaja para negociar su acceso independiente al campo de la informática y para realizar la toma de decisiones autónomas.

He aquí, a nuestro modo de ver, el principal efecto socioeconómico del impacto de las Nuevas Tecnologías de la Información y la Comunicación: la dependencia tecnológica.

Las perspectivas y consecuencias de esa dependencia ya se están evidenciando pero el alcance de sus efectos son aún desconocidos, incluso por los centros de poder dominantes.

En esta línea de pensamiento vale cuestionarse: ¿Nuevas Tecnologías de quiénes?, ¿para qué?, ¿en qué formas?, y ¿con qué consecuencias?. Es conveniente reflexionar acerca de estos fenómenos que no son exclusivamente tecnológicos, sino que inciden en el ámbito político, jurídico y social, porque integran y suplantan funciones, descalifican habilidades y modifican formas de conducta y modos de pensamiento[5].

Es necesario desarrollar iniciativas o acciones que puedan hacer viable el legítimo proceso de desarrollo de tecnologías autóctonas en nuestro país e incidir para que se logre lo mismo en la región a que pertenecemos, de acuerdo con los intereses nacionales de nuestros países, y entre estos intereses tener en cuenta especialmente los relacionados con las tecnologías más avanzadas.

■[4] AMOROSO FERNANDEZ, Yarina: "Informática como objeto de Derecho", Revista Cubana de Derecho Nº 1, 1991.

■[5] AMOROSO FERNANDEZ, Yarina: "Modernización del Derecho: Automatizar la Tradición?". Simposio de Modernización del Derecho, Villa Clara, 1994.

Frente a las nuevas tecnologías no cabe adoptar una actitud simplemente imitativa del desarrollo que en este campo han alcanzado los países más avanzados, ni tampoco una posición pasiva que conduzca a la marginación de este importante medio de progreso tecnológico. Lo que procede es concebir una manera propia de utilizarlas en el contexto de nuestros escasos recursos; sobre todo si se tiene presente que las mismas son mucho más que un instrumento, porque en síntesis constituyen la aplicación racional y sistemática de la información a los problemas económicos, sociales y políticos.

Por otra parte, no debe olvidarse que las nuevas tecnologías de la información y la comunicación son objeto de intercambio y en consecuencia pueden ser objeto de programas de integración.

Retomando el tema de las aplicaciones, debemos destacar el sinnúmero de aplicaciones que tanto desde la informática como de la telemática se han realizado y puesto al servicio de la humanidad, hacer un listado no es objeto de este trabajo, ni nos sentimos con capacidad de ello.

De manera tal que sólo aludo a la memoria colectiva, y digo, que 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, dinámico 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.

Es por todos conocido que 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.

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.

Por eso la doctrina internacional que no está al margen de esta situación; a menudo en forum especializados se ha abordado el tema; además, múltiples

organizaciones han lanzado llamadas a tomar medidas por parte de los gobiernos, para no dejar en estado de impunidad los daños ocasionados por estas acciones.

Quizá unas de las primeras acciones en este sentido fueron a iniciativa de la Federación Internacional para el Procesamiento de la Información (IFIP), quien al concluir el XI Congreso Mundial de Informática, en San Francisco, lanzó una Advertencia Mundial sobre los Virus Informáticos[6].

Por su parte en 1990, el VII Congreso de Naciones Unidas sobre Prevención del Delito y Tratamiento al Delincuente aprobó formular a la Asamblea General una recomendación en la que se insta a los Estados Miembros a dar a los funcionarios encargados de la represión de las acciones delictivas generadas en el empleo de tecnologías avanzadas de información, así como a los funcionarios de la justicia penal, una capacitación adecuada y proveerlos de medios jurídicos y técnicos suficientes para detectar e investigar[7] dichos actos.

II- ESBOZO DE ALGUNAS CONDUCTAS TÍPICAS DE LOS LLAMADOS DELITOS INFORMÁTICOS.

La protección penal de todos los posibles comportamientos indebidos realizados mediante el uso de computadoras se ha optado por dos vías:

a) la creación de tipos específicos;

b) reinterpretación de tipos penales.

En algunos casos no se excluye la segunda vía, utilizando como método legislativo la inclusión de tipos específicos a continuación de los delitos convencionales, de manera que puedan servir de punto de partida para la reinterpretación de los tipos penales tradicionales especialmente aquellos en que los actos no responden a las características típicas de ejecución de la acción, o la naturaleza del bien atacado.

En Estados Unidos, se aprobó una Ley contra el Abuso y Fraude Informático, en 1984, la que fue modificada en 1986.

■[6] Advertencia de la IFIP, San Francisco, 1989.

■[7] Documentos y Resoluciones de la ONU, VII Congreso de Prevención del Delito y Atención al Delincuente, La Habana, 1990.

En Alemania, se incluyeron figuras delictivas generadas por el uso indebido de la Informática, en la Segunda Ley para la lucha contra la criminalidad económica, de fecha de 15 de marzo de 1986.

En Austria en la Ley de 22 de diciembre de 1987, y en Francia en la Ley de 5 de enero de 1988.

En Suecia, Alemania, Francia, Austria, Estados Unidos y Gran Bretaña, se ha optado por establecer bien sea en legislaciones especiales o modificaciones al Código Penal, una tipificación legal de las conductas.

Esta fórmula ha sido interpretada como base para la creación de tipos agravados respecto de los básicos ya existentes, cuestión esta que no comparto del todo, porque el hecho de utilizarse nuevas tecnologías podría constituir un tipo agravado.

Por otra parte, ello ha llevado, también, a la reinterpretación conceptos e instituciones jurídicas; por ejemplo: "cosa" dada la inmaterialidad del software; a reconocer que no se requiere la presencia de una persona engañada para tipificar el delito de fraude o a la consideración del tiempo de máquina como "propiedad", tal como veremos en los ejemplos siguientes.

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 Lampe y más tarde Sieber proponen los siguientes tipos delictivos:

a) Fraude por manipulaciones de una computadora contra un sistema de procesamiento de datos.

Fraude informático, constituye la forma más frecuente de aparición de conductas disválidas 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.

El tratamiento legislativo al tema ha sido el siguiente:

En Suecia, se contempla la figura del fraude informático en una norma especial, y establece que "es condenable la persona que legalmente obtiene acceso a registros de datos sujetos a procesamiento o altera, destruye o ingresa esos datos en un archivo".

Con esta disposición se salvó el vacío normativo que se generaba ante la manifestación de éstas conductas, ya que la legislación penal resultaba limitada para aplicar a las mismas las figuras tradicionales de fraude y abuso de confianza.

En Gran Bretaña y Austria se sanciona penalmente "cualquier persona que ilegalmente altere, falsifique, borre o destruya cualquier material de procesamiento de datos con intención fraudulenta".

La legislación estadounidense hace constar que "todo aquel que consciente o inconscientemente acceda y, sin permiso, añada, altere, erosione, borre o destruya datos, o programas de computadora, sistema informático o red..."

En Dinamarca, Canadá y Alemania, se han introducido modificaciones en la legislación en el sentido de reconocer que no se requiere la presencia de una persona engañada para tipificar el delito de fraude.

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 Estados 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.

Internacionalmente se ha tratado el tema de la forma siguiente:

En Francia, Austria, Alemania, Suiza y Portugal se han elaborado disposiciones que están encaminadas a tratar de impedir el daño contra los bienes intangibles (datos y programas), pues a los bienes físicos se les aplica el precepto legal típico.

d) Robo de servicio.

Robo de tiempo de máquina. Utilización indebida del equipo informático o de los servicios de procesamiento de datos; bien sea "in 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 computadora.

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

Otros autores como el Dr. Julio Téllez, lo clasifican atendiendo a dos criterios: como instrumento o medio y como fin u objeto, al proponer los supuestos siguientes:

I.- Supuestos en que se utilizan las nuevas técnicas como medio u objeto.

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude).

d) "Robo" de tiempo de computadora.

e) Lectura, sustracción o copiado de información confidencial.

f) Modificación de datos, tanto en la entrada como en la salida.

g) Simulación de servicios no rendidos.

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

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

j) Uso no autorizado de programas de cómputo.

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

l) Alteración en el funcionamiento de los sistemas.

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

n) Acceso a áreas informatizadas en forma no autorizada.

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

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

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

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

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

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

Las relaciones taxativas de supuestos de actos indebidos siempre quedan incompletas, y, además, se identifican con figuras delictivas convencionales vigentes en los Códigos, 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.

Las diferencias doctrinales estriban en que varios estudiosos del tema, consideran que algunos supuestos no son otra cosa que modalidades de un mismo tipo delictivo, otros estiman que no todos las conductas pueden ser enmarcadas como delitos informáticos, 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 estiman 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 físicos, 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.

Los oponentes a la tipificación especifica, afirman que es posible ante estas conductas una aplicación de los tipos penales existentes, por medio de una interpretación teológica; argumentando que sería un tratamiento similar al seguido en el caso de hurto de electricidad, en el que fue suficiente la interpretación de ésta como "cosa".

Quizá fundado en este principio, en el Estado de Virginia se ha considerado el tiempo de máquina o de servicios de procesamiento de datos como "propiedad" y, por tanto, se incrimina su uso no autorizado.

La figura del Hacker es la principal modalidad del acceso no autorizado a sistemas de procesamiento de datos, de tal acción puede resultar la obtención ilegal de información, la destrucción de ésta o la comisión de otros actos delictivos.

La figura del (Hacker) el intruso es un ejemplo de figura clásica con respecto a las conductas indebidas nacidas de esta interacción hombre-máquina. En nuestro caso sería necesario contemplarla como delito en nuestro Código Penal.

La ley Sueca de 1983, castiga el mero acceso a un sistema de procesamiento de datos.

En Estados Unidos la "Couterfeit Access Deviece and Computer Fraud and Abuse" tipifica penalmente el acceso no autorizado a sistemas informáticos operados por el gobierno, y en particular a los asociados a la defensa nacional, los archivos externos y la energía atómica, así como a las instituciones financieras.

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.

Respecto a los daños es interesante la circunstancia de una inutilización o pérdida de su operatividad original sin implicar necesariamente la destrucción física o pérdida de su sustancia, por lo que queda demostrado una vez más que el detrimento del valor económico de un bien puede recaer sobre la sustancia material o sobre la funcionalidad de su uso.

Otro supuesto, 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 una 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.[8]

Otra de las figuras típicas de este impacto negativo de las incidencias sociales de las nuevas tecnologías de la Información y la Comunicación lo son sin duda la aparición de programas dañinos, entre los que se incluyen los virus informáticos, las bombas lógicas, caballos de Troya o tras múltiples aplicaciones informáticas, las que la jurisprudencia norteamericana ha dado en denominar Software Roger.

III.- PRESENTACIÓN 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[9], y dentro de esta denominación genérica se agrupan cuatro tipos de

■[8] AMOROSO FERNANDEZ, Yarina: Estudio: "Institucionalización de la Informática en Cuba", 1996.

■[9] AMOROSO FERNANDEZ, Yarina y GOMEZ, Mariana: "Algunas consideraciones para el estudio de la Seguridad Informática como objeto bien en Derecho", Ponencia presentada en el I Congreso de la Sociedad Cubana de Ciencias Penales, 1995.

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.

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.

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".

La Bomba del tiempo o lógica

La Bomba de Tiempo, conocida también como Bomba Lógica, es un conjunto de instrucciones que se autoejecutan en un momento determinado, dadas 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.

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 falla 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.

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[10].

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.

a) Otra consecuencia del Software Roger

La analogía entre virus informáticos y virus biológicos 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

[10] Jurisprudencia de Estados Unidos, Revista DAT.

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 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[11] 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.

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.

■[11] GUADIS, Edgar: "Enciclopedia de Virus", Laboratorio Latinoamericano contra Virus Informáticos, PII-UNESCO.

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 las 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.

b. 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" están orientadas 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 1530ª 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 acentúan 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. Quizá 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 causarán 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, a 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.[12]

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.

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

■[12] TELLEZ VALDES, Julio: "Virus Informáticos", Revista Iberoamericana de Derecho e Informática, Nº 12, 13, 14, UNED-Mérida, España.

a) comparte tiempo de ejecución;

b) comparte memoria; y,

c) 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 sería 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.

c. La distribución de los virus informáticos.

Comentario aparte merece la distribución del virus. 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, han empezado a experimentar con las instrucciones destructivas que han sido divulgadas.

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

IV - 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 esta 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. ¿Es responsable quien opera el equipo informático?

b) ¿Dónde se originó el virus? ¿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?.

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

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

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

e) ¿Qué ley deberá ser aplicada al autor del 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?

f) ¿Es el autor del virus el único responsable del daño? ¿En qué sentido puede la ley condenar a un autor de un virus que nunca tomó ninguna participación activa en su distribución del programa?

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 éste se ejecuta?.

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

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 especifico.

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, tal como veremos más adelante.

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.

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 naturales 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.

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

■[13] AMOROSO FERNANDEZ, Yarina: "Contribución al estudio del Derecho de la Informática", Curso impartido en el Escorial, España, 1995.

■[14] LAFUENTE, Jorge: "Derecho Informático", Zaragoza, España, 1992.

En los supuestos de entidades bien sean públicas 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 sistemas informáticos, ya sean usuarios directos o terceros.

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 de cada país.

En otro orden de cosas, es interesante, sin entrar con el detenimiento que el tema merece, sólo expresar que junto con estas manifestaciones 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 la Informática o la Telemática.

Entre otros elementos que gravitan sobre el llamado delito informático haciendo más difícil su detección y sanción, lo es el hecho de que un elevado numero de casos son descubiertos 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, la dificultad de detectar estas conductas debido a las condiciones y rapidez en que se pueden ser manifestadas, las dificultades técnicas para probar el cuerpo del delito y el temor de evidenciar fallas de seguridad en los sistemas de información.

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

V - CAUSAS QUE GENERAN LAS CIFRAS NEGRAS.

Varias son las causas por la cual se generan estas cifras negras. Una de ella 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 quien 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 conocidas 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, 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.

VI- LOS SUJETOS ACTIVOS O DELINCUENCIA INFORMÁTICA.

Si bien 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". Sí hay algo común: ser 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 que tienen vinculación con el ordenador.

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 retractores; mientras otros la inscriben en la delincuencia económica o como un subgrupo del guante blanco.[15]

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 Estado 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.

■[15] DEL PONT, Luis M. y NADELSTICHER, Abraham: "Delitos de cuello blanco", Cuaderno Nº 8 del Instituto de Ciencias Penales (INACIPE), México, 1981.

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 presente 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.

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 criminológica, debe sumarse una serie de variables particulares.

Entonces, ¿cómo 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.

Sólo abordaré muy sucintamente una de ellas, dada la naturaleza de este trabajo, y es el ámbito de la legislación.

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 "informáticas" acciones delictivas constituidas en nuestros códigos, sino de evaluar las características fundamentales que revisten estas actitudes y de qué modo pueden tener una respuesta legal.

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 de 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 previo 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, se debe 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 puede ser reformulados y adecuados, en tantos 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 Informatizada 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 estas que están, además, muy vinculadas a la formación del personal que enfrenta 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.

VII. UNA INTERROGANTE DEL "MAÑANA" QUE ES "HOY": ¿ES NECESARIO UNA LEGISLACIÓN 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 (...)", en nuestro caso la información digital[16].

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 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 cuáles se almacena, procesa y trasmiten diferentes tipos de información (texto, imagen y sonido) a partir de las cuales 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 cognoscibilidad 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 (...)".[17]

Así el desarrollo de la infraestructura mundial de información está transformando ya nuestro entorno común, especialmente en lo que se refiere a la

■[16] FROSINI, Vitorio: "Humanismo y Tecnología en la Jurisprudencia", Revista internagionalle de filosofía del diritto, 1965.

■[17] Bis. Cita.

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 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, en tanto 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 necesaria 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 estarnos 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 de revisar las soluciones conocidas para explorar pautas nuevas (...)"[18].

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. Por lo tanto, si bien pienso que las soluciones pueden ser logradas desde el Derecho no creo que exclusivamente desde este.

■[18] VIVANT, Michel, "Cyberespacio: ¿qué es el Derecho para las redes sin fronteras?", Conferencia Magistral, V Congreso Iberoamericano de Derecho e Informática, La Habana, 1996.

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.

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 con 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 que la humanidad tiene en el horizonte cercano[19].

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 cuales ponen en peligros 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

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

de enfrentar este reto tanto culturalmente como en un ejercicio eficiente de sus 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 Marti "Para qué sino para poner paz entre los hombres han de ser los adelantos de las ciencias".