Los "Delitos Informáticos": Situación en México

JULIO TÉLLEZ VALDÉS

Director de Estudios Superiores del Instituto de Investigación en Computación Electrónica (ICEL). Asesor de la Cámara Federal de Diputados en México. Doctor en Derecho.

1. INTRODUCCION. 2. FORMAS . 3. ORIGENES. 4. MEDIDAS NO JURIDICAS ADOPTADAS. 5. BUSQUEDA DE LA SOLUCION JURIDICA

1. INTRODUCCION.-

La problemática de los "delitos informáticos" requiere de unestudio especial en nuestro país a fin de determinar la medida en que las leyes penales vigentes constituyen un cuerpo normativo suficiente para prevenir y reprimir este tipo de conductas delictivas o si es menester la creación de figuras jurídico-penales que expresamente regulen esta nueva modalidad delictiva. Desafortunadamente, en México se ha vislumbrado incipientemente este asunto, por lo que a la fecha no ha sido tipificado ninguna conducta ilícita derivada por el avance tecnológico, pretendiendo asimilarse diversos tipos que actualmente regula el Código Penal, empero, no se debe olvidar que en materia penal no es aplicable la analogía, sino que el delito debe estar perfectamente tipificado en un ordenamiento legal, según se desprende del Artículo 14 constitucional. Aspectos tales como la integridad y seguridad alrededor de los sistemas de cómputo, son aspectos no suficientemente desarrollados, cuyas consecuenciasno se detienen en lo técnicoo en lo económico, incidiendo, de manera cada vez más acentuada, en aquello que aparentemente no tenía relación: lo legal.

2) FORMAS

Debido quizás al poder que representa los conocimientos y experiencia en materia de cómputo, y a la relativa facilidad de acceso y significativa trascendencia de la información, aunado esto a la por momentos "desorbitada" superación profesional (yo diría económica) por algunos de los que tienen el control de los llamados sistemas de información, ello a posibilitado la propensión a acciones indebidas o irregulares en las que se tienen a las computadoras como instrumento o fin. Hay quienes hablan de fraudes por computadoras, entendidosestos como el desvío de los procedimientos normales para hacer un uso indebido de los programas, alterando o destruyendo datos, los archivos, y en general el mal uso de los equipos que ocasionan pérdidas en las organizaciones. Desde luego, también se presentan otro tipo de riesgos tales como el robo de información o de programas, divulgación de claves de acceso, robo de tiempo para correr programas o conexión de equipos no autorizados, acciones que al no estar debidamente recogidas en la legislación penal, propician un incremento en cuanto a su tentativa o consecución.

3. ORIGENES

En México (sin desde luego ser limitativo en lo interno y exclusivo en lo externo), se han identificado cuatro factores que propician estas acciones:

1) El aumento del número de personas que estudian computación.

2) El aumento del número de empleados con acceso a los equipos.

3) La facilidad de uso de los equipos de cómputo.

4) El incremento en la concentración del número de aplicaciones y consecuentemente de la información. Por otra parte, según un estudio del Instituto Mexicano de Auditores Internos las causas que propician los fraudes se debe a la combinación de dos factores: el primero debido a las fallas o inexistencia de elementos de control, y el segundo, por las características propias del personalque se encuentran en situaciones inconvenientes tales como:

1) Antecedentes de deshonestidad.

2) Problemas económicos ocasionados por endeudamiento,ingresos insuficientes, nivel de vida insatisfactorio, etc.

3) Estados de ánimo contrarios a la entidad laboral, como resultado de una molestia ó frustración.

4) Rotación excesiva .

5) Falta de goce de vacaciones.

6) Personal "indispensable" para la exclusividad en el manejo de ciertos sistemas y transacciones.De aquí que la probabilidad de que las compañías puedan ser afectadas, radica en los siguientes factores:

1) La deshonestidad del posible perpetrador.

2) La oportunidad que la compañía ofrece por poseer controles inadecuados.

3) La motivación oculta de los posibles perpetradores para cometer el fraude.Los estudios realizados indicanpor tanto, que los motivos de los autores de estas acciones, son, entre otros :

1) Beneficio personal (lucro).

2) Beneficios para la organización.

3) Beneficio a otra persona o institución.

4) Rechazo a la organización.

5) Problemas financieros.

6) Deseo de sobresalir en alguna forma.Con base en lo anterior, se considera particularmente que los motivos de los empleados deshonestos y la falta de seguridad adecuada, son las causas principales para la comisión de estos delitos. A continuación se describen los sujetos del delito, como personasfísicas o morales que intervienen o que se ven afectadas:

a) El sujeto activo, usualmente identificado en los operadores, que pueden modificar, agregar, eliminar o sustituir información o programas, copiar archivos para venderlos a competidores; los programadores, que pueden violar o inutilizar controles protectores del programa, dar información a terceros ajenos a la empresa, modificar archivos, acceder a información confidencial; los analistas de sistemas, que comunmente son los únicos que conocen la operación de un sistema completo y pueden estar en colusión con los programadores u operadores; así como cualquier personal involucrado con los sistemas como el personal técnico y de servicio, los funcionarios, los bibliotecarios, hasta cualquier persona que tenga acceso a documentos o listados dejados sobre los escritorios que pueda ser vendida a competidores. Una lista publicada en los E.U.A., menciona que de 674 "criminales bancarios", recientemente detectados, 120 eran promotores de datos, 32 vicepresidentes y gerentes de operaciones, 29 funcionarios de préstamos y 14 presidentes de bancos. Desgraciadamente en México no se disponen de muchas estadísiticas sobre estos actosya que la mayoría no se llevan a juicio ni se divulgan. Sin embargo, con lo expuesto anteriormente, se puede concluír que pueden ser cometidos por personas de cualquier nivel que tengan acceso a los sistemas.

b) Los sujetos Pasivos, generalmente instituciones financieras o comerciales, y en menor medida sector público o gubernamental, en la mayoría de las ocasiones carentes de sistemas de seguridad adecuados, evidenciando que el crecimiento de los fraudes por computadora es mayor que áquel que se presenta en los sistemas de seguridad, agudizado por la escasa denuncia de irregularidades de este tipo de pérdidas, por temor a sufrir daños en la imagen corporativa, o a una posible pérdida de competitividad, clientela o confianza por parte de los mismos accionistas

4. MEDIDAS NO JURIDICAS ADOPTADAS

La falta de un adecuado o en todo caso homogéneo marco jurídico informático en nuestro país, ha motivado la implementación de distintas medidas a nivel de seguridad informáticade entre las que destacan:

a) Administración de los servicios informáticos en las organizaciones, a través de la adopción depolíticas de operación, derivadas en métodos y procedimientos de trabajo que atienden el flujo de la información, desde su origen hasta su destino final, buscando, en general, garantizar la sana operación de los recursos computacionales y los datos que estos manejan, mediante el estudio de las causas, efectos y nivel de vulnerabilidad de los diversos elementos informáticos y con ello el establecimiento de prioridades de protección.

b) Capacitación del personal usuario del equipo informático, haciéndolos sabedores de los medios o mecanismos de seguridad, formando conciencia sobre la importancia que representan los datos e información para la institución. De igual forma se busca un adecuado ambiente de trabajo para el óptimo desempeño del personal.

c) Seguridad física de los equipos, que involucra aspectos tales como el control de acceso a las instalaciones de cómputo o a sitios que albergan terminales apoyado en controles, además de la protección de instalaciones, equipos y cualquier dispositivo físico, contra desastres naturales.

d) Control técnico en cuanto al hardware o equipos y dispositivos, a través del uso de claves de identificación y autentificación del usuario.

e) Seguridad en el software, caracterizado por el adecuado desarrollo de los programas en todas sus fases, desde el diseño, la programación, la etapa de

pruebas, puesta en marcha y documentación.

f) Seguridad de los datos, mediante el ocultamiento de ciertos datos que se pueden accesar y la determinación de quién puede hacer determinado tipo de operaciones, con dispositivos identificadores que determinan qué parte de información se autoriza a utilizar y qué operaciones se pueden efectuar con ella.Aún con ello, es evidente la insuficiencia de este tipo de "reglas", aceptándose de común consenso, la urgente necesidad de creación de un adecuado marco jurídico.

5. BUSQUEDA DE LA SOLUCION JURIDICA.

Dada la desafortunada ausencia en nuestro país de un capítulo alusivo a este tipo de conductas, se ha recurrido en reiteradas ocasiones, al análisis de los distintos artículos "aplicables" del ordenamiento penal vigente, que de alguna u otra forma han sido vinculados con los llamados delitos informáticos. Así tenemos:

A) Tipos Penales Directamente Vinculados .-

a) Revelación de secretos."Art. 210.- Se aplicará multa de cinco a cincuenta pesos o prisión de dos meses a un año al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto"."Art. 211.- La sanción será de uno a cinco años, multa de cincuenta a quinientos pesos y suspensión de profesión, en su caso, de dos meses a un año, cuando la revelación punible sea hecha por persona que preste servicios profesionales ó técnicos ó por funcionario ó empleado público, ó cuando el secreto revelado ó publicado sea de carácter industrial". Consideramos que este delito se refiere principalmente a la obtención por parte de competidores de conocimientos ó elementos propios a las dos partes básicas que integran a una computadora (hardware y software), esta situación también se ve protegida tanto en su idea como en su uso no autorizado. El hardware, por su diseño, se adecúa más a la legislación patentaria (sin existir alusión al respecto) mientras que el software o programa de computación, es protegido por la Ley Autoral. Sin embargo, ambas legislaciones sólo brindan al creador, inventor o diseñador de la obra, derechos exclusivos dentro de ciertos límites temporales y geográficos. No obstante, ninguna de estas leyes son aplicables cabalmente al delito que resulta de obtener información utilizando una computadora y su posterior

divulgación por las siguientes razones: En primer lugar, una persona puede revelar "un secreto o comunicación reservada" que obtiene no con motivo de su empleo, sino por alguna computadora propia o ajena, sin tener relación laboral ni de otra clase con el sujeto pasivo. En segundo lugar, el software, al ser utilizado no se compone en su totalidad de información considerada como "obra intelectual", pues viene a ser una especie de esqueleto con espacios a llenar; una vez cubiertos, puede tratarse de información confidencial, mas no de secretos industriales ni de obras intelectuales cuya divulgación puede ser perjudicial para el sujeto pasivo más allá del tiempo que las leyes mencionadas señalan.En cuanto al hardware, éste no se vé afectado cuando una persona se introduce indebidamente desde una terminal remota e independiente al sistema de cómputo ajeno.

b) Falsificación."Art. 239.- Al que cometa el delito de falsificación de títulos al portador y documentos de crédito público, se le impondrá de cuatro a diez años de prisión y multa de doscientos cincuenta a tres mil pesos..."Art. 244.- El delito de falsificación de documentos se comete por alguno de los medios siguientes:

I. Poniendo una firma o rúbrica falsa, aunque sea imaginaria, o alterando una verdadera. II.Aprovechando indebidamente una firma o rúbrica en blanco ajenas, extendiendo una obligación, liberación o cualquier otro documento que pueda comprometer los bienes, la honra, la persona o la reputación de otro, o causar un perjuicio a la sociedad,al Estado o a un tercero. III.Alterando el contexto de un documento verdadero después de concluído y firmado, si esto cambiare su sentido sobre alguna circunstancia o punto sustancial, ya se haga añadiendo, enmendando o borrando, en todo o en parte, una o más palabras o cláusulas, o ya variando la puntuación. IV. Variando la fecha o cualquiera otra circunstancia relativa al tiempo de la ejecución del acto que se exprese en el documento. V. Atribuyéndose el que extiende el documento o atribuyendo a la persona en cuyo nombre lo hace, un nombre o una investidura, calidad o circunstancia que no tenga y que sea necesaria para la validez del acto. VI. Redactando un documento en términos que cambien la convención celebrada, en otra diversa en que varíen la declaración o disposición del otorgante, las obligaciones que se propuso contraer o los derechos que debió adquirir. VII.Añadiendo o alterando cláusulas o declaraciones, o asentando como ciertos hechos falsos, o como confesados los que no lo están, sí el documento en que se asientan se extendiera para hacerlos constar y como prueba de ellos. VIII.Expidiendo un testimonio supuesto de documentos que no existen; dándolo de otro existente que carece de los requisitos legales, suponiendo falsamente que los tiene; o de otro que no carece de ellos, pero agregando o suprimiendo en la copia algo que importe una

variación sustancial. IX.Alterando un perito traductor o paleógrafo el contenido de un documento, al traducirlo o descifrarlo; y X. Elaborando placas, gafetes, distintivos, documentos o cualquier otra identificación oficial sin contar con la autorización de la autoridad que corresponda".El aumento en el volumen y la complejidad de las actividades a realizar, han traído como consecuencia que varias de estas tareas sean efectuadas por la computadora.Por razones de orden práctico, la elaboración de documentos escritos es una de las actividades asignadas a tales máquinas.Actualmente se emiten por computadora documentos tales como cheques, letras de cambio, pagarés, facturas, etc. y, con fines de prontitud, la mayoría de éstos vienen con la firma impresa .Desafortunadamente, las características y usos de las computadoras que son utilizadas para beneficio del hombre, son las mismas que se aprovechan en su perjuicio.Así tenemos que también es práctica común la producción indebida de originales, y no de copias de los documentos mencionados.Con el uso de dichas máquinas, es relativamente fácil emitir tantos "originales" de un mismo documento como se desee, simplemente se programa a la máquina para que, por ejemplo, por cada determinada cantidad de títulos de crédito o documentos que emita, expida uno de más. Una vez realizado esto, a través de las instrucciones correspondientes, se ordena a la máquina borrar el programa mediante el cual se le dieron tales órdenes no autorizadas y de esta forma se destruya todo indicio que pueda incriminar al delincuente. Creemos que un documento indebidamente emitido por esta vía, reúne todas las características de un original, más aún cuando cuenta con la firma impresa; por lo tanto, consideramos que el tipo penal que se analiza no encuadra enteramente con esta nueva forma de delinquir. Tal vez lo que debería ponerse en tela de juicio no es la originalidad, sino la voluntad del firmante a comprometerse mediante un documento que se expide sin su conocimiento y, mucho menos, sin su consentimiento.

c) Robo."Art. 367.- Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que pueda disponer de ella con arreglo a la ley". Es cuestionable si la figura de "robo" que requiere la privación permanente de un bien mueble a la víctima se adecúa a ésta acción delictuosa porque, primeramente, este numeral habla de un "apoderamiento", mismo que debe ser material. Como ya se ha apuntado, una persona puede tener acceso desde un lugar lejano a la unidad central de procesamiento de una computadora ajena y, entre otras cosas, examinar, modificar y hasta copiar la información allí contenida ya sea por transferencia electrónica u ordenándole a la máquina que la imprima, sin que por esto exista un apoderamiento de la misma.Ahora bien, otra de las causas por las que creemos que es improcedente la aplicación de este artículo a dicha nueva conducta delictiva, es porque el robo se refiere a bienes muebles.La información es un bien intangible; es

susceptible de apropiación, pero no es mueble.Por lo tanto, si se insiste en adecuar las figuras jurídico-penales tradicionales como el robo a esta nueva modalidad delictiva, se tendrán entonces que modificar dos conceptos: el de "apoderamiento" en el que se considere no sólo el desposeimiento del bien, sino también la disminución de su valor; y el de "bien mueble" en el que se incluyan bienes intangibles como la información que sí *per se* es susceptible de apropiación, también *per se*, debe ser susceptible de protección jurídica.

d) Robo de fluído."Art. 368.- Se equiparan al robo y se castigarán como tal :I...II. El aprovechamiento de energía eléctrica o de cualquier otro fluído, ejecutado sin derecho y sin consentimiento de la persona que legalmente pueda disponer de él".Respecto a este numeral, también estimamos que es dudosa su aplicación, ya que se refiere al "aprovechamiento de energía eléctrica o de cualquier otro fluído", sin embargo, la información no es energía eléctrica ni tampoco es un fluído. El individuo que accesa a la unidad central de procesamiento de una computadora ajena, lo hace generalmente desde su terminal, por lo que está utilizando energía eléctrica a la que él probablemente tiene derecho.Por otra parte, se designa como fluído a los "cuerpos cuyas moléculas tienen poca coherencia y toman siempre la formadel vaso que los contiene", de aquí se desprende que la información no es un fluído, pues lo que fluye a través de estos sistemas es energía eléctrica y aunque la información allí contenida es representada mediante impulsos eléctricos, ésta, *per se*, no es un fluído.El acceso a una computadora ajena vía telefónica, es una de las formas más socorridas para allegarse indebidamente de información perteneciente a otras personas cuya obtención, como ya se dijo, no implica necesariamente la privación de la misma de su legítimo propietario, sin embargo, sí le ocasiona un gran daño a éste, la información pierde entonces gran parte de su valor y en algunos casos, quizá todo, con su simple divulgación. En esta acción no sólo se comete este ilícito, sino que también se desprenden los relacionados con el acceso ilegal a dicha máquina, aparte del uso no autorizado de la computadora ajena y el perjuicio que resulta para el dueño de la misma por el tiempo de servicios en que ésta es distraída para la realización de funciones no autorizadas por él.En un caso como éste, el delincuente queda impune pues el tipo penal en cuestión no es de ninguna manera aplicable a esta nueva conducta delictiva.

e) Robo de uso."Art. 380.- Al que se le imputare el hecho de haber tomado una cosa ajena sin consentimiento del dueño o legítimo poseedor y acredite haberla tomado con carácter temporal y no para apropiársela o venderla, se la aplicarán de uno a seis meses de prisión, siempre que justifique no haberse negado a devolverla, si se le requirió a ello. Además, pagará al ofendido, como reparación del daño, el doble del alquiler, arrendamiento o intereses de la cosa

usada".Consideramos que este artículo tampoco es adecuado a la conducta ilícita que resulta de accesarse a una computadora ajena, pues lo que se toma no es un bien, sino un servicio que es realizado por una máquina.Aquí el robo consiste en servicios de procesamiento, es decir, en utilizar las funciones propias de una computadora y esto ocurre frecuentemente en las empresas; esta acción es cometida por los empleados para efectuar trabajos personales utilizando dicha máquina sin autorización.Sin embargo, este ilícito también puede ser perpetrado a distancia por personas ajenas a los entes físicos o morales propietarios de las computadoras. Como ya se ha mencionado, el uso de la computadora tiene un costo en el que se implican tanto las funciones que ésta realiza (robo de servicios), como el tiempo en que las lleva a cabo (robo de tiempo), factores inseparables de la entidad física de la máquina misma.El acceso no autorizado a una computadora ajena da lugar a varias acciones delictuosas no contempladas por los tipos penales existentes, tales como:- enterarse de la información intangible allí almacenada- copiar, modificar o destruir la información que ésta contiene- realizar servicios de procesamiento. El avance tecnológico ha hecho posible la comisión de estos ilícitos y muchísimos más.La zaga negligente en la que se ha quedado el Derecho, los ha soslayado.

f) Abuso de confianza."Art. 382.- Al que, con perjuicio de alguien, disponga para sí o para otro, de cualquier cosa ajena mueble de la que se le haya transmitido la tenencia y no el dominio, se le sancionará con prisión...". Creemos que este tipo penal no encuadra cabalmente en su aplicabilidad al delito informático, toda vez que la "disposición" no recae sobre un bien mueble, sino sobre un bien intangible: la información misma que no se ajusta al concepto de "mueble" por las razones antes apuntadas al analizar el delito de robo. Por otra parte, este numeral menciona la previa transmisión de la tenencia sobre el bien que va a ser objeto de posesión, situación que no se presenta en la comisión del ilícito informático, pues el ofendido generalmente desconoce al sujeto activo que dispone de la información en cuestión, por lo tanto, no es factible la celebración de un acuerdo sobre dicha transmisión.

g) Fraude."Art. 386.- Comete el delito de fraude el que engañando a uno o aprovechándose del error en que este halla, se hace ilícitamente de alguna cosa o alcanza un lucro indebido...". Esta disposición tampoco es enteramente aplicable pues se requiere que una persona sea engañada o se dé un aprovechamiento en virtud del error en que ésta se encuentra y en el delito informático no hay tales. El sujeto activo que indebidamenteaccesa a la unidad central de procesamiento de una computadora, lo hace sin conocimiento de su propietario, por lo tanto, sin engañarlo y sin inducirlo al error.Simplemente accesa, examina, transfiere, extrae, destruye, etc., la información que ésta contiene y como intruso que

es, sale subrepticiamente. Por otra parte, en la comisión del delito informático la que es objeto de engaño es la computadora pero, cabe hacer mención que sólo las personas son capaces ante la ley, por lo tanto, "engañar" a una máquina no constituye delito...

h) Daño en propiedad ajena."Art. 397.- Se impondrán de cinco a diez años de prisión y multa de cien a cinco mil pesos, a los que causen incendio, inundación o explosión con daño o peligro a:

I...II. Ropas, muebles u objetos en tal forma que puedan causar graves daños personales.III.Archivos públicos o notariales.IV. Bibliotecas, museos, templos, escuelas o edificios y monumentos públicos, y V..."Art. 399.- Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple". Aunque estos numerales protegen a la propiedad, se refieren a ésta pero sólo en su aspecto tangible, en su integridad física . En el caso del delito informático, este tipo penal sería suficientemente aplicable ya sea para el equipo en sí, es decir, para la computadora como entidad física, como bien mueble, o para los dispositivos materiales de almacenamiento como cintas magnéticas, discos duros y flexibles, ópticos, etc. Sin embargo, este tipo penal no prevé las consecuencias que su comisión puede ocasionar en tales objetos, accesorios fundamentales de la informática, pero no en su aspecto físico, sino en el alma de su objeto, pues en caso de daño de, por ejemplo, una cinta magnética, el valor material de ésta como continente, es irrisorio comparado con el de su contenido, es decir, de la información que almacenan, cuya elaboración pudo haber implicado mucho tiempo, trabajo y dinero.

B) Tipos Penales Indirectamente vinculados.

Actualmente existen determinadas figuras contempladas en nuestro ordenamiento penal que, de acuerdo con su texto, no tienen ninguna relación con el delito informático, sin embargo, dadas las características de éste como sus resultados, estimamos conveniente la inclusión de una fracción alusiva a esta nueva conducta delictiva o la creación de un tipo penal específico.Tal es el caso de los siguientes artículos:

a) Sabotaje: "Art. 140.- Se impondrá pena de dos a veinte años de prisión y multa de mil a cincuenta mil pesos, al que dañe, destruya o ilícitamente entorpezca vías de comunicación, servicios públicos, funciones de las dependencias de Estado, organismos públicos descentralizados, empresas de participación estatal o sus instalaciones; plantas siderúrgicas; eléctricas o de las industrias

básicas; centros de producción o distribución de artículos de consumo necesario, de armas, municiones o implementos bélicos, con el fin de trastornar la vida económica del país o afectar su capacidad de defensa".Primeramente, este tipo penal sólo protege bienes y servicios públicos, de tal suerte que si se trata de bienes no pertenecientes a este sector, no constituyen el delito de sabotaje, aún si la doctrina francesa lo señala en los términos de la acción de perjuicio del obrero hacia el patrón, mediante la realización de un mal trabajo ó provocación de desperfectos en los talleres y máquinas .La Revolución Informática ha permitido que no sólo el empleado inconforme y deseoso de venganza perjudique al patrón, sino también a personas ajenas a él, ya sea con el fin de demostrar su superioridad intelectual o con propósitos terroristas, perjuicio de enormes proporciones y que puede ejecutarse a distancia; el sabotaje informático bien puede perpetrarse contra los datos, contra los programas o contra la misma computadora, y una de las formas actuales más comunes de cometerlo lo constituyen los llamados virus informáticos con la introducción de instrucciones que se infiltran automáticamente en programas y archivos, permaneciendo en la memoria de la computadora hasta en tanto no se apague, alterando o destruyendo los datos almacenados en todos los discos que se inserten en ésta, los que a su vez, quedan infectados y en posibilidad de propagar el virus, además de ocasionar otro tipo de daños, constituyéndose, por su misma dispersabilidad, en verdaderas pandemías que llevan consigo enormes pérdidas, principalmente de carácter económico.Otra de sus características,es que generalmente no hay signos visibles de infección hasta que el daño está hecho, pues el virus está diseñado para permanecer latente por mucho tiempo.Llegado el momento, se activa a sí mismo orientándose con el reloj calendario que tienen la mayoría de las computadoras; apoderándose del control de la máquina e iniciando su destrucción, por lo regular, con un "peculiar" aviso, repitiéndoseautomática e indefinidamente,sin ulteriores intervenciones.A través de estas acciones, aparte de que se ocasionan daños de enormes proporciones, los autores quedan impunes, factores que erigen paradigmas deplorables como"ejemplos a seguir", por lo que es menester que nuestra legislación contemple este tipo penal de manera urgente.

*b) Delitos cometidos por servidores públicos.*Consideramos que es necesaria la inclusión de un artículo específico al delito informático dentro del Titulo Décimo de nuestro Código Penal, pues siendo el Estado uno de los principalesusuarios informáticos, procesando inumerable y variable información de carácter fiscal, policial, político, electoral, etc., el eventual daño que puede ocasionar un servidor público al usar indebidamente una computadora, puede ser de enorme trascendencia.

"El Status de las garantías individuales: Informática y Libertad"