ALGUNAS REFLEXIONES SOBRE LA FIRMA DIGITAL Y DELITO INFORMÁTICO EN TORNO A LA "SEGURIDAD CIBERNÉTICA"

Lic. Warner Cascante Salas

INTRODUCCIÓN

A finales del año 2007, Costa Rica, uno de los países a nivel mundial que, guardando las distancias con países ricos, está en los primeros lugares en cuanto a contar con mayor cantidad de computadoras por habitante, y que incluso produce y exporta software al resto del mundo, también ha sido víctima de su avance tecnológico, cuando a varios clientes de algunos de los bancos "más seguros" del país, les sustrajeron sumas millonarias de sus cuentas corrientes y de ahorros, mediante transferencias electrónicas de fondos a través de Internet, ¡vaya precio que hay que pagar por el adelanto tecnológico! Con la llegada de la revolución científico-tecnológico, las "Tecnologías de Información y Comunicación", se han convertido en herramientas, a través de las cuales se monitorean los actos básicos de nuestra existencia como lo son las estadísticas de nacimientos y defunciones, bienes y servicios brindados por personas públicas, privadas, individuales, colectivas; el monitoreo de procesos básicos de nuestra sociedad como el control de las finanzas individuales y públicas, la comunicación formal e informal, la gestión de las diversas instituciones, industrias, administración de los programas espaciales, la producción del conocimiento y su difusión, solo para citar algunos ejemplos.

En efecto, no fue por coincidencia que la computadora fuera declarada el invento más sobresaliente del siglo XX que recién hemos dejado, ya que su impacto o incidencia en nuestra vida diaria es sorprendente y es un fenómeno que llegó para quedarse.

En consecuencia, el uso de las computadoras y por ende de las tecnologías de información y comunicación nos suministran una serie de ventajas con las cuales jamás soñaron nuestros antepasados, sin embargo, también nos planteó un reto y dilema de primer orden, como lo es el derecho del Estado a tener acceso a la información, que las diversas personas intercambiamos en la red mundial conocida como Internet, para salvaguardar situaciones de

seguridad nacional pública e incluso mundial, versus, el derecho personal a la intimidad o privacidad en las comunicaciones como derecho humano.

Es en torno al dilema seguridad pública-vrs.-derecho a la intimidad que surge el problema de la seguridad cibernética, que es el tema central del presente artículo, con dos temas estrechamente asociados que se comentarán, como lo son la denominada firma digital y el delito informático, ambos con implicaciones directas no solo en la seguridad cibernética, sino en nuestro entorno cotidiano matizado con el advenimiento de las computadoras y cuyo asidero inmanente es el uso de las tecnologías de información y comunicación.

CONCEPTO DE SEGURIDAD CIBERNÉTICA

El Diccionario de la Real Academia define el concepto **cibernética**, en su primera acepción como el "**estudio de las analogías entre los sistemas de control y comunicación de los seres vivos**".[7]

Por otro lado define el concepto **ciberespacio**, como el "**ámbito artificial creado por medios informáticos** ".[8] A su vez, conceptualiza como **cibernauta** a la "**persona que navega por ciberespacios**".[9]

En este orden de ideas, cobra relevancia la Internet [De inter, internacional y net, en inglés, red].- que se concibe como red de redes o sistema mundial de redes de computadoras interconectadas, la que, aunque fue concebida a fines de la década de 1960 por el Departamento de Defensa de los Estados Unidos; más precisamente, por la ARPA, se la llamó primero ARPAnet y fue pensada para cumplir funciones de investigación, su uso se popularizó a partir de la creación de la World Wide Web, actualmente es un espacio público o ciberespacio utilizado por millones de personas (cibernautas) en todo el mundo como herramienta de comunicación e información.

A través de la Internet se ha acuñado el concepto de "Sociedad de la Información y el Conocimiento". La definición de "sociedad de la información" implica recorrer un trayecto histórico que se profundiza a finales del Siglo XX. En este período los acontecimientos históricos, sociales, económicos y los avances científicos y tecnológicos han hecho evolucionar conceptos como "Sociedad de la Información" (Maclup), Sociedad del Conocimiento (Drucker), Sociedad Informacional y Sociedad Red (Castells) y Sociedades del Conocimiento o del Saber (UNESCO).

Manuel Castells en su libro "La dimensión cultural de Internet" define a la sociedad del conocimiento al señalar que "se trata de una sociedad en la que las condiciones de generación de conocimiento y procesamiento de información han sido sustancialmente alteradas por una revolución tecnológica centrada en el procesamiento de información, la generación del conocimiento y las tecnologías de la información".

En torno a lo anterior, tienen relevancia los temas de **gobierno electrónico, seguridad nacional y seguridad informática**, los cuales, como temas y como práctica han ido ocupando un importante espacio en el ámbito de la modernización de los estados ya sea en la gestión pública, en la relación Estado-ciudadanía o en la labor parlamentaria. El tema de gobierno electrónico como concepto comenzó a ser utilizado desde la segunda mitad de los noventa, para dar cuenta de las transformaciones que produce la incorporación de tecnologías de información y la comunicación (TIC) en el quehacer de las instituciones públicas. El advenimiento de la temática del gobierno electrónico no es casual ni espontánea, cuenta con importantes antecedentes y es parte de una tendencia internacional. El debate sobre el gobierno electrónico está vinculado a las inercias globales y a las reflexiones sobre el rol del Estado, tratándose por separado el tema de las potestades del gobierno dentro del

7 REAL ACADEMIA DE LA LENGUA ESPAÑOLA. Diccionario de la Lengua Española. Madrid España. 2001. Vigésima segunda edición. Editorial Espasa Calpe, S.A.

8 REAL ACADEMIA DE LA LENGUA ESPAÑOLA - Op. Cit.

9 REAL ACADEMIA DE LA LENGUA ESPAÑOLA - Op cit.

ámbito privado de los sujetos, vrs. el derecho a la intimidad del que hemos hablado.

Ahora bien, independientemente de las grandes ventajas y bondades de la Internet, al haberse creado ese ciberespacio, cada una de las personas que ingresa a ese ámbito artificial mundial de comunicaciones, se encuentra expuesto a una serie de fenómenos y actividades riesgosas, entre las cuales están los delitos informáticos de los cuales cualquier persona que utiliza Internet puede ser víctima, según se dirá más adelante.

En este momento del avance de las tecnologías de información, estamos frente a una situación de inseguridad cibernética o informática que ni aún los gobiernos como el de los Estados Unidos de América, que invirtió para el año 2005, la suma de 65 mil millones de dólares en Tecnología de la Información (IT) y servicios de apoyo asociados, para dar soporte a las múltiples y diversas misiones del gobierno Federal estableciendo lo que se ha dado en llamar la ***"lista de vigilancia administrativa",*** no ha logrado controlar o dominar la exposición frente a las personas que vulneran los sistemas públicos, privados, denominados "Hackers".[10]

En otras palabras, aunque pretendamos tener un ámbito de privacidad o intimidad en el que solamente ingresen determinadas personas, a través de los diversos medios, entre ellos, el correo electrónico ("e-mail"), lo cierto es que esa "privacidad" no está garantizada en forma real, ya que en un sistema operativo como por ejemplo, Windows de Microsoft, no traen en forma automática o de oficio, un bloqueo sobre la posibilidad de ingresar a la computadora como el Administrador, es decir, ese superusuario que tiene todos los privilegios para borrar archivos y programas, a menos que una persona especializada nos asesore acerca de la forma específica de crear tal bloqueo, "pequeño y minúsculo detalle" de seguridad.

A diferencia de los sistemas operativos predominantes en aproximadamente el 93% de los computadores de todo el mundo, los sistemas operativos de código abiertos, como por ejemplo Linux, toman la seguridad como una situación de primer orden, por lo que sus diversas distribuciones como Ubuntu, Suse, Knopix, Linex, Red Hat, Mandrivia, entre otros, por defecto activan la posibilidad de ser un usuario restringido y, solamente en el evento de que se requiera realizar operaciones importantes con los archivos, como borrarlos, reemplazarlos, monitorearlos, etc., el sistema solicita la creación y acreditación del superusuario, Administrador o root, de lo contrario el sistema se mantiene cerrado a cualquier incursión no autorizada o intento de vulnerabilidad, que se intente a los archivos del funcionamiento básico del sistema operativo y otros programas estratégicos para el uso del computador.

No está por demás decir que un computador sobre el cual no se han tomado las previsiones de seguridad como la configuración inicial de sus usuarios, la instalación de programas antivirus y antispyware, puede fácilmente ser dañado o vulnerado a control remoto por un Hacker, o más aun, convertir una computadora casera en un "computador zombi[11]" o esclavo el cual se puede manipular remotamente y a través de él, cometer delitos en perjuicio de terceros. En ambos casos, las consecuencias son de gran magnitud, ya que por un lado, los virus informáticos destruyen mediante el borrado o la alteración de las rutinas de programación, programas estratégicos de un computador. Por su parte, los spyware, son programas de monitoreo remoto cuya función es extraer información del computador de la víctima, datos vitales del equipo y de sus usuarios, como por ejemplo las direcciones de Internet que se visitan, las teclas más comunes que son digitadas, las claves más frecuentes que se digitan, entre ellas las bancarias y otros sitios en los que

10 Evans, Karen. Oficina de ADMINISTRACIÓN Y PRESUPUESTO. Declaración Administradora de Gobierno Electrónico y Tecnología de la Información Oficina de Administración y Presupuesto ante el Comité sobre Reforma de Gobierno de US House of Representatives abril de 2005.

11 Entiéndase como tal aquel computador sobre el cual su propietario pierde el control y es manejado remotamente por otra persona sin permiso de su propietario. La consecuencia más grave de un computador zombi es que por medio de este se pueden cometer ilícitos cibernéticos sin conocimiento ni autorización de su propietario.

se requieren datos personales de identificación. Como respuesta a este fenómeno de inseguridad cibernética, se crea el concepto y herramienta denominado "Firma Digital", el que abordaremos de inmediato.

FIRMA DIGITAL

La firma digital nació como respuesta o reacción técnica a los problemas de vulnerabilidad en la información, así como a las infracciones a nuestra intimidad o privacidad en las comunicaciones. Mediante ésta, se pretende proteger la integridad de los datos contenidos en determinado documento electrónico, con el fin de que el destinatario tenga la plena certeza acerca de la autoría de dicho documento electrónico.

En el caso de Costa Rica, con la promulgación de la Ley de Certificados y Firmas Digitales y Documentos Electrónicos, Nº 8454, y su reglamento promulgado mediante Decreto Ejecutivo No. Nº 33018-MICIT, la interrogante contenida en uno de nuestros artículos, que en su momento publicamos, mediante el nombre ¿Tiene validez probatoria el documento electrónico?([12]), ya se ha disipado en forma definitiva. En efecto, aunque hace pocos años, algunos nos atrevimos a indicar que el documento electrónico sí podría tener validez probatoria, lo cierto es que hoy, el contenido de los cuerpos normativos indicados, establecen sin lugar a dudas y con meridiana claridad la confirmación de nuestra tesis.

Ahora bien, somos conscientes de que el problema de fondo no se resuelve únicamente dictando leyes, sino que a la par de éstas, hay que crear una verdadera cultura de seguridad en cada uno de los usuarios de las tecnologías de Información y comunicación, de otra manera, caeríamos en la ingenuidad que Platón, el filósofo griego, señaló en su obra La República, y que varios han dado en llamar el *"platonismo de las reglas"*, es decir, creer ingenuamente que basta con crear leyes para que los vicios humanos se erradiquen, no obstante, es con lo que hay que trabajar hoy día. En este momento de la exposición se impone reflexionar sobre los alcances y contenido de la firma digital según la ley costarricense aprobada en el 2005, en ese sentido, iniciaremos indicando que la ley No. 8454 define la firma digital como:

> ***"...cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico. Una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado."***

En cuanto a su equivalencia señala:

> ***"Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y la eficacia probatoria de su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita. Los documentos públicos electrónicos deberán llevar la firma digital certificada."***

También sobre el concepto de equivalencia funcional en los documentos, en el artículo 3 señala:

> ***"Cualquier manifestación con carácter representativo o declarativo, expresada o transmitida por un medio electrónico o informático, se tendrá por jurídicamente equivalente a los documentos que se otorguen, residan o transmitan por medios físicos. En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación, se entenderán de igual manera tanto los***

12 Oficina de Contraloría de la Universidad de Costa Rica, Boletín Técnico Año V Número 1-2001

electrónicos como los físicos. No obstante, el empleo del soporte electrónico para un documento determinado no dispensa, en ningún caso, el cumplimiento de los requisitos y las formalidades que la ley exija para cada acto o negocio jurídico en particular."

De conformidad con las tres normas transcritas que están contenidas en la Ley de Firma Digital costarricense, se puede apreciar un gran esfuerzo legislativo que luego de varios años de recolección de información y consulta a los profesionales de las tecnologías de información y comunicación, ha sintetizado los elementos básicos que se esperan de un mecanismo como la firma digital, a saber, a) el otorgamiento de carácter probatorio a un documento electrónico firmado digitalmente, b) la equivalencia funcional o equiparación de un documento firmado digitalmente a uno firmado manual o convencionalmente, y c) la autoridad y responsabilidad del Estado de orquestar y tutelar esta nueva dinámica, para evitar una anarquía o especulación con este importante tema de la seguridad cibernética, acerca del cual, las diferentes legislaciones a nivel mundial, apenas comienzan a dar sus primeros pasos en el establecimiento y persecución de conductas delictivas en materia informática, según se desarrollará en el siguiente aparte, específicamente el caso de Costa Rica.

DELITO INFORMÁTICO

Paralelamente a la creación de una legislación sobre firma digital, la legislación costarricense, visualizó de igual importancia la modernización y actualización de la legislación penal sobre el tema, por ello se abocó a la creación de la figura penal denominada delito de fraude informático, en ese sentido la legislación costarricense creó ese delito de la siguiente manera:

Sobre el delito de fraude informático: El artículo 217 del Código Penal señala:

"Se impondrá prisión de uno a diez años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema."

En sentido amplio, el delito informático es cualquier ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o como fin. Como medio, en el caso del fraude informático, y como fin, en el sabotaje informático (artículo 229 bis del Código Penal).

Por su parte, el National Center for Computer Crime Data de los Estados Unidos de América indica que:

"el delito informático incluye todos los delitos perpetrados por medio del uso de ordenadores y todos los delitos en que se dañe a los ordenadores o a sus componentes."

De igual forma, y siempre con ese carácter de generalidad y amplitud, la Organización para la Cooperación y Desarrollo Económico (OCDE) explica que el "delito informático es toda conducta ilegal, no ética o no autorizada, que involucra un proceso automático de datos y/o la transmisión de datos".

Asimismo, William Cashion –estadounidense experto en informática– señala que el "delito informático es cualquier acto inicuo que no puede ser cometido sin un ordenador o que no existiría sin un ordenador o su tecnología" (citado en "Delitos informáticos, Carlos Chinchilla Sandí, Farben, 2004, página 27).

Si bien para la comisión de un delito informático se requiere un ordenador, ello no implica que siempre que en la comisión del hecho delictivo esté presente un computador, estaremos en presencia de un delito informático. Para mostrar un caso obvio, si se violenta un

cajero automático para sustraer el dinero que guarda, no se cometerá un delito informático.

De acuerdo con la redacción de la norma en el Código Penal vigente, la acción del sujeto activo consistirá en influir en el procesamiento o el resultado de los datos de un sistema de cómputo, a través de varias conductas como afectar el procesamiento o resultado de los datos mediante manipulación de la información, alimentar el sistema de forma irregular; estos son actos que incidirán en el proceso de los datos, es decir, en la realización de las instrucciones de un sistema. Para ampliar un poco más el concepto, un ejemplo más concreto sería el siguiente: en el proceso de pagar el salario a los empleados hay una serie de pasos a seguir; si alguno se altera fraudulentamente, incidirá en el resultado del proceso, obteniéndose productos incorrectos o falseados por estas acciones.

El usuario aparece al final de ese proceso, y en términos generales, no lo puede o debe modificar. Para hacerlo, requiere el ingreso al sistema, y usualmente debe poseer ciertos conocimientos y atribuciones jurídicamente otorgadas. Las personas que cometen delitos informáticos presentan algunas características que no tiene el común de las personas, como la destreza en el manejo de los sistemas informáticos, una posición estratégica que le facilita el manejo de información restringida, o, en muchos casos, ambas condiciones ventajosas.

Este tipo de ilícitos caen dentro de la categoría comúnmente llamada "delitos de cuello blanco". Estos delitos, por lo general, requieren un alto grado de especialización del que los comete por la tecnicidad en el manejo de los sistemas, por encontrarse protegidos por mecanismos de defensa cuya vulneración requiere, usualmente, de conocimientos técnicos.

"Esta predisposición de medios defensivos en forma general y la limitación que se puso a los delitos electrónicos nos permite inducir en forma clara que para ingresar a cualquier sistema sin la debida autorización (para el caso la simple intrusión resultaría el delito subsidiario de otros más graves como hacking o robo de información, por citar algunos) implica necesariamente vencer una resistencia predispuesta del sistema colocada allí expresamente por razones de seguridad, –según expresan los programadores y constructores–." (Derecho Penal Informático, Gabriel Cámpoli, Investigaciones Jurídicas S.A., 2003, página 28).

Según indica el doctor Chinchilla Sandí, dentro de esas conductas destacan la manipulación de los datos de entrada: conocido también como sustracción de datos, que es el más común en vista de la facilidad para la comisión y la dificultad en el descubrimiento. No requiere de conocimientos técnicos en informática y puede realizarlo cualquier persona que tenga acceso al procesamiento de datos en su fase de adquisición; manipulación de programas: difícil de descubrir pues el sujeto activo (así llamado en el derecho penal) ha de tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en introducir nuevos programas o nuevas rutinas. Un método muy usado es el denominado "Caballo de Troya", el cual: "Consiste en introducir dentro de un programa de uso habitual, una rutina o conjunto de instrucciones, no autorizadas, para que dicho programa actúe en ciertos casos de forma distinta a como estaba previsto.

"Así, en determinadas circunstancias puede ejecutar erróneamente un cálculo, por ejemplo, desviando partidas hacia cuentas ficticias. También podría perseguir la impresión de documentos no autorizados o no imprimir documentos reales. Es frecuente utilizar este método para introducir una modificación al programa de tratamiento de cuentas corrientes de manera que cada vez que se consulte el saldo de una determinada cuenta lo multiplique por una cantidad aumentando el cupo y permitiendo la autorización de pagos o transferencias por un importe muy superior al saldo real.

"No obstante ser muy difícil de detectar, ya que el programa normalmente funciona en forma correcta, es vital

el implantar técnicas de prevención."[13]; manipulación de los datos de salida: se lleva a cabo fijando un objetivo al funcionamiento del sistema informático, como el fraude a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos, lo que se hacía con tarjetas bancarias robadas. Ahora se usa equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y en las tarjetas de crédito. Como se observa, la conducta implica cierto manejo de los datos, los programas, que incide en el proceso de los datos del sistema, con lo cual se configura la conducta penalmente reprochable conocida como delito informático. Como corolario de estas reflexiones, debemos señalar que paralelamente a la comodidad que nos brindan las tecnologías de información y comunicación, están los riesgos que en materia de seguridad cibernética se asocian. Que como una respuesta a esta patología tecnológica que vulnera derechos fundamentales de los ciudadanos como el derecho a la intimidad sea en su computador personal o en el computador central de una institución en la que conste esa información privada, algunas legislaciones de varios países, entre ellos, Costa Rica, han iniciado con la creación de un mecanismo de seguridad como lo es la Firma Digital y el establecimiento o creación del delito de fraude informático, al menos como paliativos o soluciones parciales a este gran problema de seguridad informática, problema al fin y al cabo de nuestros días, ¡viva la tecnología! ▲

13 Herrera Bravo, Rodolfo. "Reflexiones sobre la delincuencia vinculada con la delincuencia digital (basada en la experiencia chilena)". En: http://rodolfoherrera.galeon.com/refxdel.pdf