Revista Academia y Virtualidad

Rol del derecho penal y la informática forense en la protección de la información en la era disgital [1]

Role of criminal law and computer forensics to protect information in the digital age

Autores:

Beitmantt Geovanni Cárdenas Quintero
BGCardenasQ@udistrital.edu.co

Hilma Ximena Fonseca Ruíz
hilma.fonseca@unimilitar.edu.com

Fecha de presentación: agosto 2012
Fecha de aceptación: octubre 2012

Resumen

El mundo moderno, dominado por las tecnologías de la información y las comunicaciones, ha permeado todos los espacios de interacción del ser humano, su auge y expansión a dado origen a la denominada "sociedad digital", eje de progreso y desarrollo en el mundo actual.

Cuello (2005) refiere que la tecnología modificó todos los hábitos de los individuos en el mundo, lo primero que hace cada uno al levantarse es mirar el reloj, encender la radio o Tv y luego prender el PC.

Pero no todo es positivo, el avance tecnológico trae aparejada la aparición de las más variadas conductas delictivas propias de este desarrollo avasallante. Como consecuencia de esta realidad, se requiere implementar técnicas y estrategias para la identificación y control de los riesgos que se ciernen sobre los datos y la información dado su incalculable valor, en esta tarea juega rol activo la legislación penal y la informática forense.

Palabras clave:

Derecho penal, informática forense, seguridad, protección, era digital, delito.

1. Artículo de reflexión.

Revista Academia y Virtualidad

Abstract

The modern world penetrated by information and communication technology has pervaded any area of human interaction; its rise and expansion led to the so-called “digital society”, currently a progress and development axis in the world. Cuello (2005) says that technology has changed every habit of individuals in the world

But not everything is positive since any technological progress brings the most varied criminal conduct typical of this huge development. As a consequence of this reality, it is required to implement techniques and strategies in order to identify and control risks posed to data and information, given its untold value, where criminal law and computer forensics play a critical task.

Keywords:

Crime, criminal law, digital age, computer forensics, security, safety.

Introducción

Sin duda alguna, la evolución arrolladora en ciencia y tecnología que presenciamos desde hace algunas décadas, ha traído crecimiento y desarrollo para la humanidad, pero al mismo tiempo, ha traído efectos nocivos que han obligado a todos los actores sociales (individuos, organizaciones y Estado) a tomar medidas para hacer frente a esta realidad.

En el caso particular de las organizaciones modernas interesadas en propender por una mayor efectividad y eficacia en sus acciones, que quieran ser competitivas y busquen un posicionamiento en el mercado, deben estar prestas a realizar un blindaje informático como punto de partida para afrontar la incertidumbre, la complejidad y el cambio que trae consigo la era digital.

En el plano económico, un ejemplo sencillo muestra la realidad actual, las empresas virtuales crecen y se multiplican, sin requerir como antaño de un espacio físico para funcionar, abarcando más mercado, llegando a un mayor número de clientes y a lugares tan remotos inimaginables para el comercio tradicional. Las relaciones comerciales sustentadas en transacciones electrónicas se convierten en el motor del mundo. Para Hernández (2000) la transformación de datos (sonido, texto y video) son las bases del comercio electrónico en la aldea global.

El raudo avance tecnológico y la inmersión en la era digital ofrece innumerables beneficios, pero a la par trae diversas conductas atentatorias de los derechos de individuos, organizaciones y sociedad en general.

Revista Academia y Virtualidad

Los ataques a la información y los datos son el pan de cada día, a raíz de esta situación se violan derechos constitucionales fundamentales, se atenta contra la intimidad y la honra, se vulnera la dignidad humana, se desconoce el derecho de habeas data, sólo por mencionar, algunos ejemplos de la situación actual.

En este sentido, este artículo analiza la protección y seguridad de la información como imperativa, y exigencia de primer orden para las organizaciones modernas, el análisis se circunscribe al rol que juega el derecho penal y la informática forense frente a este escenario. Los delincuentes informáticos se multiplican, los riesgos aumentan y la necesidad de defensa a la información es incuestionable.

1. La sociedad de la información

Desde el punto de vista histórico, ya de tiempo atrás, en el informe publicado por la UNESCO el 16 de agosto de 1976, se presentó de manera clara y ante la comunidad internacional la importancia que en las próximas décadas tendría la información.

Márquez (2002) dice en referencia a este documento, "lo fundamental de tal informe es que culminó, en cierto modo, los esfuerzos sociales emprendidos para lograr el reconocimiento general de los derechos fundamentales de la información".

La sociedad de la información es expresión de las realidades y capacidades de los medios de comunicación en renovarse y evolucionar, merced a los desarrollos tecnológicos que se consolidaron a partir de la última década del siglo pasado: la televisión, el acopio de información, la propagación de video, sonido y textos, a podido comprimirse en soportes de almacenamiento como los CD, a través de señales que no podrían conducir todos esos datos si no hubieran sido traducidos a formatos digitales. La digitalización de la información es el sustento de la nueva revolución informática, su expresión hasta ahora más compleja e impactante es la Internet.

En este sentido refiere (Perot, 1995), el impacto de las nuevas tecnologías de la información y la comunicación (TIC) conlleva dos dimensiones: de un lado la dimensión informativa a la que corresponden los sistemas de información (SIATD, ERPs, Datamart, Datawarehouse, CRM) y del otro lado la dimensión comunicativa que comprende medios digitales como (web, intranet, correo electrónico, IM, Foros, SMS), el intercambio inmediato de altos volúmenes de información y el desarrollo de medios emergentes de comunicación llevaron al desarrollo de las "redes".

El avance, crecimiento y expansión de las tecnologías de la información y las comunicaciones (TIC), en el nivel científico, académico, empresarial y técnico, implica para la sociedad, para los entes del Estado y para las organizaciones en general, un compromiso grande, un estar alerta, un estar atento frente a los riesgos y amenazas que este desarrollo conlleva. De cara a este contexto se han tomado diferentes medidas en aras de proteger este bien valioso (la información y los datos), de un lado la informática forense (IF) y del otro la legislación penal.

2. La informática forense (IF) frente a la protección de la información

La informática forense tuvo su origen en Estados Unidos hacia 1984 en las agencia de inteligencia Norteamérica (FBI). Se define la IF como la ciencia que se encarga de identificar, adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional.

Revista Academia y Virtualidad

Se denomina tratamiento automatizado a aquellas operaciones y procedimientos técnicos de carácter mecanizado o no, que permiten la recolección, grabación, conservación, modificación, bloqueo y cancelación, así como la cesión de datos que resulten de comunicaciones, consultas e interconexiones y transferencias.

El valor de la información en la sociedad y sobre todo en las empresas es cada vez más importante para la supervivencia, posicionamiento y crecimiento en el mercado. La necesidad de implementar su uso, adquiere cada vez mayor relevancia, a través de ella se garantiza la efectividad de las políticas de seguridad y de protección tanto de la información como de las tecnologías que facilitan la gestión de este activo en las organizaciones.

La informática forense investiga los sistemas de información con el fin de detectar y poner en conocimiento evidencias de vulneración. Se debe utilizar inicialmente con una finalidad preventiva, de tal manera que sirva a las empresas para auditar y controlar los riesgos antes de que ocurran, a través de la práctica de diversas pruebas técnicas, por medio de mecanismos de protección instalados, y en general, a través de las condiciones de seguridad aplicadas a los sistemas de información.

Esta ciencia permite detectar los riesgos de seguridad para corregirlos oportunamente, a nivel organizacional con la redacción y promulgación de oportunas políticas y estrategias sobre uso de los sistemas de información, se hace frente a esta problemática, la que incluye divulgación y aprensión de estos derroteros en el talento humano de la empresa, adicionalmente se requiere implementación de esas políticas, a través de medidas concretas que propendan por preservar y proteger la información contenida y manejada por la compañía en todos sus niveles. La IF es una herramienta útil de detección, con los resultados que arroja su ejecución se alimenta el sistema empresarial, legal y social y se prevé la comisión de las más variadas conductas atentatorias de los intereses de la organización.

De otro lado, cuando la seguridad de la empresa ya ha sido vulnerada, la informática forense permite recoger rastros probatorios, para averiguar siguiendo las evidencias electrónicas, el origen del ataque, si es una vulneración externa o interna de la seguridad, si se ha presentado alteraciones, manipulaciones, fugas o destrucciones de datos en la empresa, y así según el evento, establecer las medidas de intervención.

Las distintas metodologías forenses propenden por la recolección segura de datos de diferentes medios digitales y evidencias, sin alterar los datos de origen, si se encuentra alguna vulneración o mal procedimiento, este no tendrá ninguna validez dentro de un proceso legal.

Cada fuente de información debe ser catalogada y luego analizada. Las evidencias digitales deben llevar a un dictamen claro, conciso, fundamentado y con justificación de las hipótesis planteada, coherente con el material probatorio recaudado. Con procedimientos claramente predeterminados se identifican, aseguran, extraen, analizan y presentan pruebas emanadas electrónicamente para ser sustentadas dentro de un proceso.

Todo el procedimiento debe desarrollarse según disponen los requerimientos legales para no vulnerar derechos de terceros. Ello para que llegado el caso, las evidencias sean aceptadas por los jueces y puedan constituir un elemento de prueba fundamental, siempre y cuando hayan sido llevadas al proceso según lo dispone la Constitución y las leyes colombianas.

Revista Academia y Virtualidad

La importancia de la informática forense se detecta en el aumento creciente del valor de la información en las organizaciones, en el uso que se le está dando a la información dentro y fuera de las empresas, en el desarrollo de la internet y en el uso permanente de los PC en las empresas y en la vida personal de cada individuo.

Gracias a la informática, las organizaciones obtienen solución a sus problemáticas de privacidad, competencia desleal, hurto de información confidencial y espionaje, conductas que se presentan como consecuencia del uso indebido y malintencionado que algunas personas están haciendo de las nuevas tecnologías de la información.

Cabe destacar que el objetivo fundamental de la IF es proteger la información antes, durante y después de sufrir alguna vulneración.

La información, al constituirse en el bien o activo más valioso en la vida moderna, debe blindarse y protegerse de manera que quienes deseen atentar contra ella sean disuadidos de cometer la conducta delictiva, a través de la ejecución de medidas de seguridad coherentes con los avances tecnológicos que trascienden el día a día.

3. Legislación y seguridad informática

De otro lado y persiguiendo el mismo fin de protección a la información, encontramos al derecho penal. En el caso de Colombia la ley prevé el delito informático desde el año 2009[2], como bien jurídico tutelable. Lima (2007) refiere "el delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como medio o fin".

El delito informático para Rivera (1999) es entendido, como aquella conducta ilícita realizada a través de computadoras empleadas como instrumento o medio y como fin u objetivo.

Como instrumento o medio

Se refiere a las conductas delictivas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito. Por ejemplo, cuando utilizan las computadoras para efectuar falsificaciones de documentos de uso comercial. En la actualidad las fotocopiadoras pueden hacer copias de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.

Como fin u objetivo

En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física. El caso se presenta cuando por ejemplo se alteran datos contenidos en documentos almacenados en un ordenador.

2. Ley 1273 de 2009. Por medio del cual se crea un nuevo bien jurídico tutelado, denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Revista Academia y Virtualidad

Las cifras sobre criminalidad en materia de delitos informáticos en Colombia, salieron a la luz pública con la promulgación de la ley 1273 del 5 de enero de 2009*, conductas que no obstante su frecuente y repetida ocurrencia quedaban antes de la promulgación de la ley en el completo anonimato, el avance en tecnología informática en pos de la automatización de tareas o al menos facilitación del trabajo, trajo consigo el nacimiento de las más variadas formas de criminalidad cibernauta.

En este sentido, las nuevas tecnologías de la información y las comunicaciones dispone de herramientas informáticas y telemáticas que permiten la manipulación de la información, creando espacios propicios para la violación y vulneración de este bien jurídico, día a día se asumen riesgos y se enfrentan nuevos peligros consecuentes con el medio tecnológico en el que nos desenvolvemos, es por esta razón, que toma relevancia el derecho, como respuesta a esta nuevo contexto de desarrollo. Frente a esta circunstancia, la legislación penal de Colombia consagró la protección del bien jurídico de la información y los datos.

Con la relevancia actual de la información automatizada, el interés de la reserva o intimidad se ha desplazado de la protección del sujeto humano, individuo o grupo a la protección del objeto, al banco de datos personales, sobre el cual hoy se ejerce el *right to privacy*.

Las organizaciones son perjudicadas y lesionadas por un sujeto que utiliza el PC, ya sea como medio o como fin para la comisión del delito, vulnerando intereses jurídicamente tutelados como la intimidad, el patrimonio económico, la fe pública, la autonomía personal, el derecho de *habeas data*, el buen nombre etc.

Méndez (2011) refiere al respecto, los ciberataques contra entidades y compañías no son nuevos ni escasos. De hecho el general Keith Alexander director de la Agencia Nacional de Seguridad de Estados Unidos, le dijo a la agencia Reuters que los computadores del pentágono reciben 250 ataques todos fallidos cada hora.

El bien jurídico tutelado en los delitos informáticos es la información y los datos, en cuanto a su calidad, idoneidad y veracidad, señala Herrera (1998).

El bien jurídico nace de una necesidad de protección y se torna penal sólo si reviste una importancia fundamental, o sea cuando las condiciones sociales a proteger sirvan de base a la posibilidad de participación de los individuos en la sociedad.

Quien atenta contra este bien jurídico es denominado por la ley penal sujeto activo, generalmente es una persona con habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

El sujeto pasivo o víctima del delito, (por ejemplo una organización) es el ente sobre el que recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los “delitos informáticos”, mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos.

La norma colombiana, Ley 599 de 2000 Código Penal (CP) contempla la protección de la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. En la actualidad los nuevos sistemas de información no sólo se utilizan como

Revista Academia y Virtualidad

herramientas de soporte a las actividades humanas sino como un medio eficiente para obtener y conseguir información. En este orden de ideas, se tipificó como conductas delictivas el acceso abusivo a un sistema informático (artículo 269A del CP), la obstaculización ilegítima de sistema informático o red de telecomunicación (artículo 269B del CP), la interceptación de datos informáticos (artículo 269C del CP), el daño informático (artículo 269D del CP), el uso de *software* malicioso (artículo 269E del CP), la violación de datos personales (artículo 269F del CP), y la suplantación de sitios web para capturar datos personales (artículo 269G del CP).

En este escenario, se atenta contra la confidencialidad de los datos y de la información cuando, por ejemplo, se revela información referente a la vida personal, patrimonial o crediticia que poseen los individuos y las corporaciones y que ha sido guardada en un base de datos. Se vulnera esta confidencialidad cuando se utilizan programas no autorizados para alterar dañar, copiar, eliminar o impedir el uso de datos almacenados en sistemas de información, como cuando se modifica dolosamente una base de datos de un sistema de información dentro de una organización, cuando se "chuzan" líneas telefónicas, cuando hay intromisión indebida en sistemas de información o bases de datos ajenas, cuando se utiliza indebidamente claves de acceso y nombres de usuario, cuando se explora la memoria de un computador para obtener datos que posteriormente se usan dolosamente y con fines ilícitos.

Se atenta contra la integridad de la información y los datos cuando se usan las bombas lógicas, los virus informáticos, cuando se falsifica un documento electrónico, creando el escenario propicio para alterar archivos en su extensión, eliminándolos o multiplicando archivos desconocidos dentro de todo el sistema.

Se atenta contra la disponibilidad de la información y los datos como en el bombardeo de correos electrónicos, cuando se impide a alguien dolosamente el acceso aun sistema de información o a una base de datos.

El derecho penal castiga la conducta dolosa, es decir la intención de causar daño que tiene el sujeto activo de esta conducta, dejando de lado elementos de la culpa como la negligencia, la impericia o la falta al deber de cuidado.

El hurto por medios informáticos (artículo 2691 del CP) y semejantes y la transferencia no consentida de activos (artículo 269J del CP), es una conducta delictiva que en la realidad se presenta cuando, por ejemplo, se digita una clave para realizar una transacción por internet o cuando se paga servicios por bancamóvil, el cibercriminal copia la clave y posteriormente cuando se trata de ingresar nuevamente se ofrece una página del banco pirateada muy similar a la verdadera, se ingresa los datos y en ese instante el delincuente tienen acceso a la cuenta, la cual desocupa, hurta en poco tiempo, generalmente transfiriendo estos activos a otra cuenta.

Por ello, se recomienda observar muy bien la página accedida, la dirección *web* y el candado de seguridad, cuando la organización realice movimientos financieros por Internet.

A nivel punitivo como se ha visto, se han conseguido importantes avances en materia de regulación normativa en cuanto a seguridad y protección de la información y los datos, sin embargo, no todo debe dejarse en manos del Estado. Los usuarios de las TIC tienen compromisos y obligaciones por cumplir, las organizaciones deben tomar medidas a este respecto, algunas muy sencillas como, mantener un antivirus instalado en todos los PC de la empresa,

Revista Academia y Virtualidad

recomendar a los empleados no dar clic de manera inconsciente en cualquier enlace que aparezca en su PC, así ingresan virus informáticos, que abren la puerta a los intrusos para que estos tomen control del equipo y lo vuelva un zombi a su servicio.

Otra medida importante que debe tomar la compañía, consiste en que su personal no sea excesivamente confiado con los sitios web que visitan, por ejemplo, no es correcto realizar consultas, transferencias de fondos o cualquier tipo de transacción desde computadores diferentes a los proveídos por la empresa. La página donde se digitan los datos debe manejar información encriptada, lo que se reconoce cuando la dirección cambia a http y se observa un candado en la barra de direcciones del navegador. Algunas empresas no dan mayor preeminencia a esta situación, ni toman las medidas de rigor, ya sea por desconocimiento o por exceso de confianza, poniendo en riesgo este bien valioso de la información y los datos. Recordemos una frase muy citada en la actualidad, "quien tiene la información tiene el poder".

La realidad descrita ha impulsado y promovido a la ciencia del derecho para generar todo un sistema protector de este bien jurídico. Como señala Márquez (2002), penalmente se considera relevante ese valor económico de la información como activo de primer orden, susceptible de custodia y defensa. Así las cosas, el derecho penal y la informática forense constituyen una excelente herramienta de defensa de la información y los datos en la organización. El mundo de la tecnología es muy dinámico, las conductas delictivas evolucionan, frente a esta realidad incuestionable, el derecho y la informática no pueden quedarse rezagados; deben asumir su rol como instrumentos adaptables e innovadores, flexibles y de avanzada, brindando a la comunidad y sociedad en general, seguridad informática coherente con el contexto de cambio y evolución permanente propio de la modernidad.

Desde esta óptica, es necesario que todas las organizaciones interesadas en prosperar y ser competitivas, tomen conciencia de la necesidad inaplazable que tienen en torno, al establecimiento de acciones efectivas que protejan su información, fijando políticas, estrategias, y programas que cumplan con este objetivo. El departamento de seguridad debe mirarse no como una opción en la empresa sino como una necesidad imperiosa, frente a las crecientes amenazas que trae consigo la inmersión en la era digital.

Referencias bibliográficas

1. Cuello, G. (2005). Derecho y tecnologías de la información. Bogotá. Editorial Superintendencia de Sociedades.

2. Cuervo J. (1997) Un nuevo desafío jurídico: Los delitos informáticos. Uruguay. Editorial Universal.

3. GIGA (2000). Delitos Informáticos: Protección Penal de la Intimidad. La Habana.

4. Gómez M. (1994). Delincuencia informática patrimonial", in "Informática y Derecho, pág. 455.

5. Hernández, G. (2000) comercio electrónico. Bogotá. Ediciones librería central.

6. Herrera R. (1998). Reflexiones sobre los delitos informáticos motivados por los desaciertos de la ley chilena N. 19223. Publicado en internet en http//publicaciones.derecho.org/redi/No.05 diciembre de 1998/herrera.

7. Lima L. (2007) El delito electrónico. Editorial Ariel.

Revista Academia y Virtualidad

8. Márquez C. (2002).El delito informático. Bogotá. Editorial leyer.

9. Méndez J (2011). Los hackers en pie de guerra. en Enter.co Colombia.

10. Perot, A. (1995). ¿Qué es la informática jurídica?. Buenos Aires. Editorial social.

11. Rivera, A (1999). Dimensiones de la informática en el derecho. Bogotá. Editorial Jurídica radar.

12. Romero M. (1988). Poder Informático y Seguridad Jurídica" Madrid Editorial cosmos

13. Téllez J (1996). Derecho Informático. México. editorial MC Graw Hill

14. Ulrich, S (2000). Los delitos informáticos en el Derecho Español, in Informática y Derecho pág. 483.

15. Unesco (cit por Márquez 2002) El delito informático.

Perfil de los autores

Beitmantt Geovanni Cárdenas Quintero

Ingeniero de Sistemas, especialista en ingeniería de *software*, Magister en ciencias de la información y las comunicaciones, con énfasis en sistemas de información, docente de la Facultad de ingeniería en el área de posgrados de Proyectos informáticos, investigador del grupo Gestión de Proyectos Informáticos GEPRINFO, en líneas de inteligencia artificial, gestión de conocimiento y gestión de proyectos de ingeniería. Correo electrónico: BGCardenasQ@udistrital.edu.co

Hilma Ximena Fonseca Ruiz

Administradora de empresas y abogada, especialista en higiene y salud ocupacional y en instituciones jurídicas, Magister en Derecho. Docente y miembro del Grupo de investigación PROPPIO de la Facultad de Estudios a Distancia de la Universidad Militar Nueva Granada. Correo electrónico: hilma.fonseca@unimilitar.edu.co.