Prevención Versus Fraude: La Auditoría Informática

EMILIO DEL PESO NAVARRO
Banco Hipotecario
(ESPAÑA)

Es mejor prevenir los delitos que punirlos.
Cesare Beccaria (De los delitos y las penas).

INTRODUCCION

El pensamiento de CESARE BECCARIA es aplicable, por supuesto, a todo el ámbito del Derecho Penal pero, si cabe, aún más al específico dominio de los llamados delitos informáticos como trataremos de explicar en las líneas que siguen.

En los últimos años el uso de las nuevas tecnologías de la información en las empresas y en las distintas Administraciones ha experimentado un desarrollo espectacular.

En un período de cambio acelerado e intenso, en un mundo, como lo denomina TOFFLER, de la tercera ola o del superindustrialismo (TOFFLER 1985) el gerente, el empresario ha de revisar todas las conjeturas de la gerencia sobre el mundo económico y social que le rodea y esto sólo puede hacerlo disponiendo de una información actual y veraz.

Por ello el empresario, el gestor de nuestros días demanda una información cada vez más actual y elaborada para poder tomar decisiones más rápidas y con menos riesgos.

Dado el volumen de datos que es preciso manejar para elaborar esa necesaria información en un tiempo prudencial antes de que quede obsoleta, ya no son válidos los métodos tradicionales de tratamiento de la información. Es necesaria la utilización de las nuevas tecnologías que permitan ese masivo tratamiento de datos con una alta velocidad de proceso.

El empleo de sistemas más o menos informatizados es usual en la mayoría de las grandes y medianas empresas y con la aparición de los ordenadores personales y los paquetes integrados su introducción en las pequeñas crece rápidamente.

El uso de estas nuevas tecnologías ha generado importantes beneficios, pero también ha creado nuevos riesgos ya que hoy en día la información es uno de los patrimonios más valiosos de la empresa y por ello hay que protegerla contra una amenaza que cada día cobra más fuerza: la utilización de estas nuevas tecnologías con fines delictivos.

Es importante resaltar el gran valor que en nuestra época adquiere la información. Siempre ha sido valiosa, pero en el pasado no existía la posibilidad como ocurre ahora, de convertir informaciones parciales y dispersas en informaciones en masa y organizadas.

RIESGOS POTENCIALES DE LA INFORMACION

Esta importancia acrecienta los riesgos que amenazan a la información y hace que las consecuencias que su pérdida origina puedan llegar a ser catastróficas. En el pasado, por ejemplo, el incendio de la biblioteca de Alejandría fue una pérdida cultural irreparable, pero forzoso es reconocer, como dice el profesor SCALA, que no afectó a la vida política, económica o social de Grecia y Roma. Por el contrario la información que hoy se elabora automáticamente y se archiva en los computadores es algo vivo, cambiante, dinámico y directamente relacionado con la actividad humana. En definitiva es un bien que debe ser protegido, porque su destrucción acarrearía daños a personas e instituciones.

La facilidad de borrado y de reescritura sobre los soportes magnéticos los hacen especialmente sensibles a la alteración, supresión o introducción de datos dejando escasas huellas de la manipulación o la absoluta ausencia de ellas. (Scala 1990).

Para tratar de evitar los riesgos potenciales que el uso de estas nuevas tecnologías en la empresa trae consigo o por lo menos minorizar sus desastrosas consecuencias nace la Auditoría Informática, como veremos mas adelante.

Es importante resaltar la velocidad con que, a diferencia de lo que ocurre en otro tipo de delitos, puede desaparecer la prueba cuando se comete un fraude informático. Desaparición que en algunos casos puede llegar a ser, como se ha dicho, total sin dejar prácticamente ninguna huella.

Esta circunstancia habremos de tenerla necesariamente en cuenta cuando tratemos de implantar algún sistema de prevención.

Existen tres momentos claves en el procesamiento de la información en los que ésta puede ser alterada: en el momento de la entrada de los datos en el sistema, durante el tratamiento de los mismos en esa «caja negra» que es el ordenador, entendido en su más amplio significado, y en la salida de datos del sistema.

Con los sistemas tradicionales de auditoría se pueden verificar la entrada y salida de los datos pero dificilmente se puede comprobar lo que ocurre durante el procesamiento de los mismos.

Para nadie es un secreto que una salida impresa o por pantalla de un terminal puede ser perfectamente «dibujada» a conveniencia de quien lo hace con la posibilidad de falsear la realidad.

La integración de la Informática, en particular gracias a las redes, hace el problema todavía más grave; las consecuencias de una anomalía pueden propagarse al exterior de las empresas e incluso alcanzar a los usuarios individuales. Las implicaciones sobrepasan, por tanto, al simple plano socioeconómico, y alcanzan a la propia ética.

UNA NUEVA FORMA DE DELINCUENCIA

La proliferación en los últimos años de los sistemas informáticos en el mundo empresarial y en el de las diferentes Administraciones Públicas ha propiciado la aparición de una nueva forma de delincuencia. Sin asumir riesgos físicos ni ejercer violencia ahora es posible obtener, de forma fraudulenta, ingentes cantidades de dinero sin dejar rastro y con la seguridad de que en el caso de ser descubiertos se gozaría de una total impunidad al no estar contempladas estas nuevas figuras delictivas en el ordenamiento jurídico español.

Al estudiar esta problemática es muy interesante tener presente la motivación del delincuente informático. Existe un paralelismo entre los motivos para cometer «delitos comunes» y «delitos informáticos» aunque en el segundo caso no esté empleada la palabra delito con propiedad. Los objetivos de ganancia personal causada por necesidades económicas o ganancia institucional para beneficiar a una empresa, o incluso el deseo de venganza en contra de una compañía, aunque por métodos diferentes, son aplicables a ambos tipos de delitos.

Hay, sin embargo, motivos específicos propios de la existencia de los ordenadores. El ordenador se presta al juego de la exploración y con su tecnología es un reto a la inteligencia humana.

No es fácil encontrar estadísticas fiables sobre estos crímenes contra la propiedad y sobre el coste que para las empresas supone esta actividad delic-

tiva, pues al tratarse principalmente de entidades del mundo financiero, no son muy proclives a airear este tipo de información, por el resultado negativo que para el negocio podría suponer la disminución de clientes temerosos de una hipotética falta de seguridad de la entidad.

Objetivo de esta nueva forma de delincuencia son tanto los datos como las diferentes aplicaciones de los sistemas informáticos.

La gravedad del problema es tal que en un futuro se podría llegar a la eliminación por medios informáticos de un competidor, que no estuviese debidamente protegido, creando criminalmente el caos en su sistema informático y originando con ello la desaparición de su empresa.

Perfil del delincuente informático

En el delito que nos ocupa no hay un tipo de delincuente único con características propias y definidas, no existe un «retrato robot» y el panorama es amplio y variado, desde el ratero aficionado, al administrativo furtivo, pasando por el timador casual y por el niñato adolescente y desocupado, hasta llegar al profesional astuto, que emplea medios sofisticados para alcanzar un lucrativo fin. (LAFUENTE 1990).

El delito informático en el párrafo anterior es entendido en un sentido muy amplio.

Es interesante el perfil del delincuente informático que propone Luis Camacho en un dominio más restringido del delito informático y en función de la información recogida en un cierto número de fraudes descubiertos:

-Suele ser empleado de confianza, bien por el tiempo que lleva en la empresa o bien por el tipo de trabajo que realiza.

-Es un empleado que por su trabajo tiene acceso al sistema informático y conoce suficientemente sus debilidades como para permitirle realizar el hecho delictivo.

-En gran número de casos suele ser usuario del sistema y no técnico informático. Es conveniente tener presente que este perfil se ha logrado en función de los fraudes descubiertos, por lo tanto esta afirmación puede ser debida más que a un nivel superior de honradez del colectivo de técnicos, a la posibilidad de que los fraudes que cometen sean más difíciles de descubrir.

-Suele ser una persona que trabaja en solitario o como máximo en grupo de dos o tres personas.

-Carece de antecedentes penales.

-Joven con edades comprendidas entre 18 y 30 años, varón, en su mayoría soltero y sin ataduras familiares.

-Profesional brillante y altamente motivado por su profesión y por el desafio técnico que conlleva. (CAMACHO 1987).

Es conveniente resaltar en este perfil la característica de que el presunto delincuente suele trabajar en solitario, esto viene a confirmar que aún la criminalidad organizada no ha entrado a operar en el mundo informático, lo cual no quiere decir que no lo haga en el futuro.

IMPORTANCIA DEL ESTABLECIMIENTO DE UN SISTEMA PREVENTIVO

El perfil descrito nos lleva a la conclusión de que gran parte de los fraudes informáticos son cometidos desde dentro de las propias empresas bien por empleados que siguen trabajando en la misma empresa, bien por personas que en el pasado trabajaron en ella y por lo mismo conocen su sistema informático.

El establecimiento de un sistema de evaluación informática periódico, en el aspecto preventivo, suele producir efectos positivos inmediatos, pues el conocimiento por parte del personal de una empresa de que se efectúa regularmente una evaluación de este tipo evita en gran proporción la comisión del «delito» informático ante la posibilidad de ser descubierto con facilidad.

Aún más positivo sería el establecimiento de un sistema de evaluación contínuo, que evitaría los tiempos muertos entre una evaluación y la siguiente.

LA AUDITORIA INFORMATICA

Este sistema de evaluación, que con carácter preventivo, se propone en el párrafo anterior en realidad es lo que se conoce como Auditoría Informática.

Para entender mejor lo que es la Auditoría Informática vamos a seguir la definición, muy completa, de RAMOS GONZÁLEZ:

«La Auditoría Informática comprende la revisión y la evaluación independiente y objetiva, por parte de personas independientes y técnicamente competentes del entorno informático de una entidad, abarcando todas o algunas de sus áreas, los estándares y procedimientos en vigor, su idoneidad y el cumplimiento de éstos, de los objetivos fijados, los contratos y las normas legales aplicables; el grado de satisfacción de usuarios y directivos; los controles existentes y un análisis de los riesgos.» (RAMOS GONZÁLEZ 1990).

Como vemos uno de los objetivos de la Auditoría Informática, y para nosotros como juristas el más importante, es evaluar la fiabilidad de los sistemas informáticos en cuanto a la exactitud de los datos o información que trata a través de los diferentes controles existentes.

Estas revisiones abarcan no sólo los sistemas implantados sino algo todavía más importante, aquellos sistemas que estan en desarrollo.

En el momento del desarrollo de las aplicaciones se deben prever ya determinados controles que posteriormente puedan ser rastreados por los programas de auditoría.

DIFERENTES ASPECTOS DE LA AUDITORIA INFORMATICA

La Auditoría Informática la debemos, pues, contemplar en sus dos aspectos: como posible medida de prevención, en algunos casos de disuasión, para que algo no ocurra y como medida de fiscalización para comprobar lo que ha ocurrido y en su caso facilitar la necesaria prueba.

El empresario actual debe imitar a aquella casada prudente que antaño elevaba una oración al Cielo a fin de que su marido no la engañase, una segunda para que si la engañaba no llegase a tener conocimiento de ello y una tercera para que si la engañaba y se enteraba no le importase. El empresario debe rogar en primer lugar para que en su empresa, en su sistema informático no se cometa un fraude, en segundo lugar para que si se comete se pueda detectar y en tercer lugar para que si lo anterior ocurre se pueda lograr una prueba del fraude cometido. Nos atrevemos a decir que debería seguir rogando para que el fraude cometido, descubierto y probado estuviese a su vez tipificado como delito en el Código Penal.

Si importante es la labor de prevención, en la que queremos hacer hincapié no lo es menos, cuando ésta fracasa, esa otra labor de fiscalización.

Si en cualquier tipo de delito es importante recoger la prueba del mismo lo antes posible y siempre con anterioridad a su temida desaparición; en el caso del fraude informático esto es vital por la facilidad que existe para que las pruebas sean borradas intencionadamente o sin intencionalidad, simplemente por la dinámica del sistema.

CONCLUSIONES

Lo expuesto anteriormente nos lleva a la conclusión final de que la Auditoría Informática puede perfectamente servir para **prevenir, descubrir y probar** el hasta el momento fraude informático y que esperamos que en un futuro próximo sea delito informático.

La razón por la que en el dominio de los llamados delitos informáticos es más aplicable el pensamiento de Beccaria, mejor prevenir que penar, que en otro tipo de delitos, viene motivada, con independencia de sus derivaciones de tipo filosófico, por la práctica inexistencia de unas normas legales que castiguen los mismos, lo que, a la postre, viene a significar el disfrute de una total impunidad.

Insistimos en que el simple conocimiento de que en una empresa se dispone de las debidas medidas de seguridad en sus instalaciones y se realizan las Auditorías Informáticas precisas, es la mejor medida de prevención frente al fraude informático y la inversión que se realice en este área será una de las más rentables para la empresa.

Es evidente que, poco a poco, el empresario, el gestor va comprendiendo la utilidad y la necesidad de contar con los auditores informáticos.

Los juristas no los debemos olvidar, pues su trabajo nos puede ser de gran utilidad.

De forma inexorable, en un futuro próximo, las empresas que no puedan tener la certeza de que sus sistemas informáticos son fiables, que sus datos responden a la realidad, que no son víctimas de estos nuevos tipos de criminalidad no podrán competir en ese gran mercado del mundo superindustrial que se avecina y tenderán a desaparecer.

Todo esto es trasladable a la diferentes Administraciones Públicas, aunque en éstas, obviamente, el resultado final no pueda ser el mismo.

Quisiera terminar estas modestas líneas con una reflexión del gran pensador español Julián Marías muy apropiada para los que de una forma u otra nos movemos en este fascinante mundo de la Informática:

«Es menester que los que usan la tecnología electrónica no crean que los aparatos piensan por ellos, es esencial que vean que la técnica electrónica da solamente instrumentos para pensar yo, único que puede hacerlo, único que puede saber.(Marías 1985).

BIBLIOGRAFIA

BECCARIA BONESANA C. «De los delitos y las penas». Madrid. *Aguilar* 1969. 121 pp. (p. 180).

CAMACHO L. «El delito informático». Madrid 1987. 162 pp. (p. 84).

LAFUENTE J. J. «Conozca las artes de los delincuentes informáticos». Estrategia Financiera núm. 57, 1990. (p. 22).

MARÍAS J. «Cara y Cruz de la Electrónica». Espasa Calpe. Colección Austral. 1985. 103 pp. (p. 99).

RAMOS GONZÁLEZ M. A. «Contribución a la mejoría de las técnicas de Auditoría Informática mediante la aplicación de métodos y herramientas de Ingeniería del Conocimiento». Tesis Doctoral. Madrid Universidad Politécnica 1990. 119 pp. (p. 17).

SCALA ESTALELLA J. J. «Validez legal de los documentos generados por sistemas automáticos». Encuentros sobre Informática y Derecho 1990-1991. Facultad de Derecho e Instituto de Informática Jurídica de la Universidad Pontificia de Comillas (ICADE). Pamplona. *Aranzadi* 1992. (p. 11).

TOFFLER A. «La empresa flexible». Espluges de Llobregat. Plaza y Janés 1990. pp. 220 (p. 103).