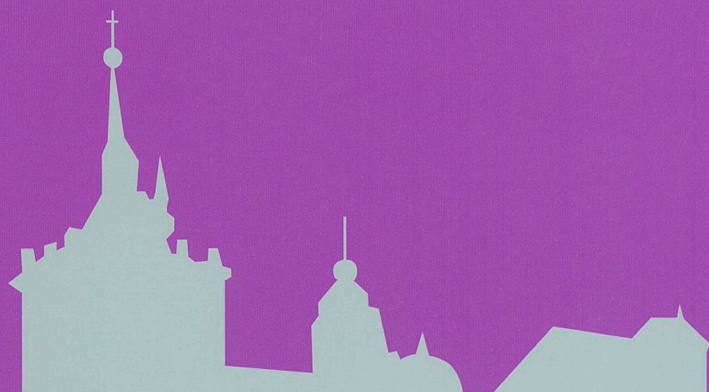




# PRESENTE Y FUTURO DE LA SEGURIDAD EN LA SOCIEDAD DE LA INFORMACIÓN



PUBLICACIONES  
DE LA FUNDACIÓN POLICÍA ESPAÑOLA  
Colección Estudios de Seguridad

Edita: Fundación Policía Española

Conde de Aranda, 16, 3ª planta

e-mail: iep@dgp.mir.es

Coordinador Editorial:

Salvador Cantero

Equipo Editorial:

Manuel Aguilar, Francisca Romero, Elena Valiente y Juan Moreno

Equipo de Traducción:

Subdirección General del Gabinete Técnico

Corrector:

Francisco J. Meco

Imprime: Tecnología Gráfica

Maquetación: Félix Gil

D.L.: M-22198-2004

Todos los derechos reservados.

No se permite la reproducción total o parcial de este libro,  
ni su incorporación a un sistema informático, ni su transmisión en cualquier forma  
o por cualquier medio, sea éste electrónico, mecánico, reprográfico,  
gramofónico u otro, sin el permiso previo y por escrito  
de los titulares del copyright.



## ÍNDICE

<u>PRESENTACIÓN</u>	7
<u>CONFERENCIA INAUGURAL</u>	9
- <b>Agustín Díaz de Mera y García Consuegra</b> <i>Director General de la Policía</i>	11
<u>PRIMER PANEL</u>	19
<u>LA SOCIEDAD DE LA INFORMACIÓN Y MARCO JURÍDICO</u>	
- Redes y sociedad de la información <b>Félix Requena Santos</b> <i>Catedrático de Sociología de la Universidad de Santiago de Compostela</i>	21
- Ciberespacio: limitaciones jurídicas y procesales <b>Alberto Dorrego de Carlos</b> <i>Director General para la Modernización de la Administración de Justicia</i>	39
- Iniciativas políticas europeas para mejorar la seguridad de la sociedad de la información <b>Danny de Temmerman</b> <i>Administrador, Dirección General de la Sociedad de la Información, Unión Europea</i>	55
- Sociedad de la información y seguridad <b>Manuel Aguilar Seco</b> <i>Inspector del Cuerpo Nacional de Policía</i>	63
- Normativa española y comunitaria <b>Noelia García Noguera</b> <i>Abogada especialista en nuevas tecnologías</i>	73
<u>SEGUNDO PANEL</u>	101
<u>VULNERABILIDADES Y CIBERAMENAZAS</u>	
- Delincuencia tecnológica <b>Miguel García Izquierdo</b> <i>Comisario del Cuerpo Nacional de Policía, Jefe de la Unidad Central de Inteligencia Criminal</i>	103
- Ciberterrorismo: una aproximación al problema <b>Juan Hidalgo Cuesta</b> <i>Comisario del Cuerpo Nacional de Policía, Vocal Asesor del Secretario de Estado de Seguridad</i>	119
- Ciberespacio y delincuencia organizada <b>Francisco Aranda Guerrero</b> <i>Comisario del Cuerpo Nacional de Policía, Jefe de la Oficina Central Nacional (INTERPOL)</i>	131

- La delincuencia virtual en la Unión Europea. Valoración y evolución del fenómeno <b>Ian Casewell</b> <i>Analista de EUROPOL</i>	141
- Los puntos críticos tecnológicos en los sectores productivos <b>Bernardino Cortijo Fernández</b> <i>Vicepresidente de Seguridad de Terra</i>	159
<u>TERCER PANEL</u>	171
<u>PROTECCIÓN, DETECCIÓN Y RESPUESTA</u>	
- Iniciativas públicas del Ministerio de Ciencia y Tecnología en el ámbito de la seguridad de la información y las comunicaciones <b>Salvador Luis Soriano Maldonado</b> <i>Subdirector General de Servicios de la Sociedad de la Información Ministerio de Ciencia y Tecnología</i>	173
- Hacia una cultura de seguridad tecnológica <b>Adrián Moure Lledó</b> <i>ASIMILEC</i>	183
- Centros de alerta temprana, un modelo de colaboración <b>Antonio Amador Reyes</b> <i>Inspector del Cuerpo Nacional de Policía Jefe de Grupo de Seguridad Lógica</i>	193
- Protección de la tecnología <b>Javier Pericacho Sastre</b> <i>Inspector Jefe del Cuerpo Nacional de Policía</i>	201
<u>COLOFÓN</u>	211
- Colofón <b>Isaac Martín Barbero</b> <i>Director del Seminario</i>	213



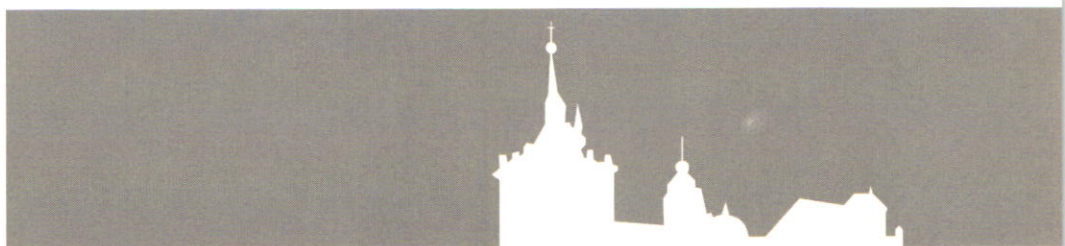
## ***Presentación***

Entre los días 7 y 11 del mes de julio de 2.003, se celebró en el marco de los Cursos de Verano de El Escorial que organiza la Fundación General de la Universidad Complutense, el seminario "Presente y futuro de la seguridad en la Sociedad de la Información".

Este seminario evidencia la sensibilidad, la necesidad de analizar, de buscar respuestas y señalar tendencias, especialmente en el campo de la seguridad, ante la nueva sociedad que las tecnologías de la información están configurando y moldeando.

Es manifiesto que las tecnologías, son absolutamente necesarias y contribuyen decisivamente al desarrollo y evolución de la sociedad. También es cierto que su aplicación, su uso masivo y acelerado está alterando las estructuras clásicas de protección y respuesta que venían funcionando hasta ahora. Alteración que genera oportunidades hábilmente aprovechadas por la delincuencia y cuya actuación no sólo causa daños materiales sino desconfianza y preocupación en la sociedad. Desconfianza que constituye un lastre para el desarrollo y el crecimiento que verdaderamente tienen esas tecnologías de la información y la comunicación.

Para conocer mejor el entorno tecnológico que se está configurando, los déficits en seguridad que conlleva; evaluar los riesgos; identificar las oportunidades y concretar respuestas, especialmente la ofrecida por el Cuerpo Nacional de Policía, se organizó este seminario que dirigido por Isaac Martín Barbero, Director del Instituto de Estudios de Policía de la Subdirección General del Gabinete Técnico de la Dirección General de la Policía, contó con la encomiable labor de los miembros de dicho Instituto.



## CONFERENCIA INAUGURAL



# **EL CUERPO NACIONAL DE POLICÍA: UNA GARANTÍA DE SEGURIDAD PARA EL DESARROLLO DE LA SOCIEDAD DE LA INFORMACIÓN**

**AGUSTÍN DÍAZ DE MERA Y GARCÍA CONSUEGRA**  
**Director General de la Policía**

11

Concurro en este impresionante marco de San Lorenzo de El Escorial para inaugurar el curso que este verano organiza la Dirección General de la Policía gracias al apoyo moral y económico de nuestros patrocinadores, al entusiasmo de muchos hombres y mujeres de dentro y de fuera de nuestra casa y gracias, por supuesto, a la estrecha colaboración que mantenemos con esa insigne Institución que es la Universidad Complutense.

Concurro, digo porque de un rápido repaso al programa del Curso se desprende que los temas y los ponentes que esta semana hemos concitado pujarán y con fuerza, por su interés y atención. Con todo, puesto que me corresponde el privilegio de abrir el ciclo, recojo el guante con ilusión y en la convicción de que muchas de las ideas que quiero compartir con ustedes ni les serán nuevas ni les dejarán indiferentes. Bien al contrario, todos los presentes somos conscientes de que del modo y manera en que le demos respuesta a algunos de los interrogantes que la Sociedad de la Información nos plantea dependerá, en gran medida, el porvenir de eso, que sin miedo al tópico, podemos calificar como la Sociedad Global. Esta sociedad, del mañana, tiene muchas vertientes y muchos ámbitos, unos de mayor importancia que otros pero en todos, la seguridad -entendida como la dimensión que define la ausencia o presencia de riesgos- constituirá un elemento de especial interés.

## **¿QUÉ ES LO NUEVO DE LA SOCIEDAD DE LA INFORMACIÓN?**

La historia tiene pocas constantes y son muchos los que en la búsqueda de éstas han naufragado en quimeras. Sin embargo, dos rasgos sí han demostrado un importante valor explicativo. La persistencia del "cambio" y su continua aceleración.

La superación de la materialidad, la territorialidad y centralidad que se inició con el advenimiento de la Era Industrial se ha visto reforzada en la Era de la Información. Como señala Nicolás Negroponte, las cuatro virtudes cardinales de la Sociedad de la Información —descentralización, globalización, armonización y capacitación— erosionan sin cesar las limitaciones impuestas por el espacio y el tiempo.

Hoy resulta posible acceder más lejos, más rápido y con menor coste a cualquier punto de lo que fue nunca antes. Cada vez más intersticios de la vida cotidiana e institucional son penetrados por las tecnologías de la información. Este entorno genera oportunidades, pero sin duda también amenazas. En la medida en la que crece la interdependencia, también lo hacen las vulnerabilidades.

12

## **¿POR DÓNDE EMPEZAMOS A CONSTRUIR UNA SOCIEDAD DE LA INFORMACIÓN MÁS SEGURA?**

En la concepción de una respuesta eficaz a los desafíos que para la seguridad presenta la Sociedad de la Información, ha de primar la identificación de sus vulnerabilidades y el modo en que pueden ser explotadas por sujetos (individuos o grupos) en los que confluye el ánimo de causar daño con su capacidad de producirlo. En definitiva, la respuesta ha de comenzar a elaborarse desde una adecuación de las tareas de inteligencia.

La realidad actual impone desafíos nuevos a la actividad de inteligencia. El análisis estratégico se ve afectado por la dificultad de hallar la continuidad necesaria en un entorno permanentemente cambiante; el análisis táctico, tan vinculado a la identificación de las particularidades espaciales y geográficas, requiere una redefinición en un ámbito virtual; por último, el análisis operativo y dentro de éste la capacidad para determinar la autoría, se complica de modo evidente en los nuevos entornos.

La ciberinteligencia debe tener como fin prioritario la acumulación de información necesaria para entender los actuales y futuros comportamientos en la red. Por ello, la inteligencia debe transformarse para mantener su capacidad de identificar amenazas y contraamenazas, vulnerabilidades y respuestas frente a éstas, así como los motivos y desencadenantes de los comportamientos de las conductas de los agentes.



En todo caso, la ciberinteligencia debe partir de dos premisas: no existe prácticamente ningún aspecto de la vida moderna que no mantenga una dependencia directa o indirecta respecto de la red y, por otra parte, la inteligencia sólo puede ser efectiva si se da un grado suficiente de sensibilidad frente a las ciberamenazas y éstas son tomadas en serio. En otras palabras, una inteligencia efectiva requiere transversalidad en el diagnóstico y consciencia de seguridad para su eficacia.

Deseo detenerme un momento en este último punto. Resulta capital profundizar en la cooperación entre las distintas administraciones y las empresas, en el común propósito de concienciar a la sociedad sobre la importancia de la ciberseguridad y la conveniencia de compartir conocimientos en este campo.

La ciberseguridad debe reforzarse en todos los ámbitos, frente a posibles agresiones exteriores pero también contra ataques interiores. El diseño de los sistemas, su gestión y la mejora de la formación en materia de seguridad del personal constituyen aspectos básicos de una nueva estrategia de ciberseguridad.

## **¿CUÁL ES EL PELIGRO AL QUE NOS ENFRENTAMOS EN LA ERA DE LA INFORMACIÓN?**

13

El Equipo de Respuesta frente a Emergencias Informáticas (CERT en sus siglas en inglés) de la Universidad Carnegie Mellon registró entre 1996 y abril de 2003, 217.394 incidentes de seguridad. A pesar de que esta cifra subestima el número real de los incidentes, resulta llamativo que, si por terrorismo entendemos actos públicos de violencia o sabotaje generadores de temor u horror en los "oponentes", los apocalípticos pronósticos que veían en la Red un campo propicio para la sucesión de ataques terroristas han errado, ya que ni uno solo de estos incidentes mereció la calificación de terrorista.

Probablemente, los terroristas han comprendido que la capacidad de los "ataques virtuales" para desafiar el poder de los Estados o intimidar a los ciudadanos es todavía hoy limitada. A menos que vengan acompañados simultáneamente por ataques físicos que produzcan daños "reales", los ataques "virtuales" tendrán poca incidencia material y temporal, por el momento.

Nadie debe inferir, de lo anterior, una trivialización de la cuestión. Bien al contrario, las cosas podrían cambiar en la medida en la que las sociedades extiendan la presencia de las redes informáticas y las empresas y entes gestores de infraestructuras descansen más en Internet y sus protocolos. Cualquier evolución en este sentido que no se corresponda con

una mejora de la seguridad, constituirá una inquietante fuente de nuevas amenazas.

### **¿ENTONCES CUÁLES SON LOS CAMPOS EN LOS QUE LA SEGURIDAD DEMANDA UNA ACTUACIÓN MÁS URGENTE?**

A la hora de ofrecer una respuesta de seguridad a una realidad espacial y temporal concreta se impone partir de unos supuestos que reflejen la realidad a la que nos enfrentamos. En este caso, el nuevo marco es temporalmente dinámico y geográficamente global.

Las tendencias que hoy se hacen presentes y habrán de continuar en los años venideros son:

- La difusión de la tecnología.
- La expansión mundial de redes comerciales en los campos del transporte, la información y las finanzas.
- La aparición de nuevas formas de organización.
- La pérdida de relevancia de las fronteras nacionales.
- La decreciente eficacia de las políticas en ausencia de coordinación y cooperación.

Por lo que se refiere a la incidencia de estas tendencias sobre el delito sólo identificaré dos:

- El empleo de la globalización como un elemento multiplicador del impacto y/o beneficio de las acciones criminales.
- El incremento de la importancia de la detección y la prevención frente a la represión, por lo que toca a la eficacia de la acción de los Cuerpos y Fuerzas de Seguridad del Estado.

Estas realidades se van traduciendo por la vía de los hechos en una cristalización del cibercrimen como una realidad en la que cobran preponderancia, siquiera numérica, cuestiones referidas a la delincuencia común y organizada y no tanto materias de seguridad nacional.

Sentado este planteamiento permítanme concentrarme por un momento en el cibercrimen, entendido por tal, tanto aquellos "delitos informáticos" como otros delitos más tradicionales cometidos empleando ordenadores y tecnología de red.



A pesar de que por razones comerciales, fundamentalmente el miedo a perder la confianza de sus clientes, muchas empresas ocultan información sobre hechos delictivos cometidos sobre sus sistemas de tecnología de la información o redes de comunicación, en el año 2000 el FBI estimaba que las pérdidas mundiales debido al ciberdelito alcanzaban los 10.000 millones de dólares anuales.

Aunque muchos de los ciberdelitos tienen un origen interno, en la variada serie de criminales de la Era de la Información encontramos "hackers", "crackers", diseñadores de virus, narcotraficantes, pedófilos, estafadores, grupos de crimen organizado...

Con ánimo de lograr cierta sistematización no exhaustiva podemos subsumir esta realidad en dos grades grupos:

1.- Delitos informáticos o de redes.

- Intrusismo.
- Piratería.
- Pornografía infantil.
- Denegación de servicio.
- Fraudes con tarjetas de crédito.
- Robo de contraseñas.

15

Los casos de los virus "I love you" (10.000 millones de dólares en daños) o "Melissa" (80 millones de dólares) constituyen ejemplos paradigmáticos de la velocidad a la que crece el poder destructor de estos criminales.

2.- Ciber-fraude y e-delitos:

De la mano del desarrollo del mercado electrónico han venido, los intentos de efectuar ciberrobos, manipular mercados de valores.

Sin embargo, la Sociedad de la Información también ofrece vías para mejorar la seguridad.

A pesar de todo lo anterior en la Dirección General de la Policía desde muy pronto comprendimos que el ciberespacio nos brindaba herramientas e instrumentos para combatir el crimen en todo su amplio espectro.

La ubicuidad de la informática nos lleva a tener presente en cada actuación las posibilidades que nos ofrece a la hora de recabar elementos probatorios y ello nos impone obligaciones de conocimiento a la hora de luchar contra las organizaciones criminales.

En el terreno de la inteligencia, la interconexión de los miembros del Cuerpo Nacional de Policía -hoy no hay un puesto policial sin Inter-

net corporativa- permite además de una actualización y coordinación constante, un ágil acceso e intercambio de las bases de datos.

En el trabajo de la Policía Científica la irrupción de la informática ha supuesto una auténtica revolución. Los métodos de medida, control y análisis, el tratamiento de la imagen, los sistemas de identificación visual, los de reconocimiento de impresiones digitales, de identificación genética, identificación de voz o de armas de fuego, han sufrido todas drásticas modificaciones que han multiplicado su eficacia y, en la mayoría de los casos, siguen ofreciendo importantísimos recorridos de mejora en los próximos años.

En el área de la seguridad ciudadana, la utilización de las posibilidades de la cartografía digital sólo ha comenzado a arrojar sus prometedores frutos.

Por lo que toca a la eficaz gestión de la información, acrónimos como SIDENPOL, PERPOL, SIG, se han convertido ya en lugares comunes para los hombres y mujeres del Cuerpo Nacional de Policía, y son contemplados como herramientas de trabajo básicas en los que descansan políticas y proyectos ambiciosos como por ejemplo, la entrada en vigor de los denominados "juicios rápidos" iniciados el 28 de abril de 2.003.

16

Por último, no querría abandonar el terreno de la utilización que la Dirección General de la Policía ha hecho de las nuevas tecnologías sin mencionar el importante esfuerzo desplegado para acercarnos al ciudadano con la puesta en funcionamiento de la Oficina Virtual de Denuncias.

Así, en la gestión, en la inteligencia, en la prevención, en la investigación, en la prueba y en la atención al ciudadano podemos todos en el Cuerpo Nacional de Policía sentir un orgullo legítimo por habernos situado en la vanguardia de la comprensión y utilización de las novedades que han surgido de la mano de la Sociedad de la Información. Me resta por lo tanto, compartir con ustedes lo que creo que son nuestros actuales desafíos.

## EL FUTURO EMPIEZA HOY

Debemos partir de una premisa fundamental: gran parte del crecimiento económico y la prosperidad hecha posible por la revolución de las Tecnologías de la Sociedad de la Información está aún por materializarse y la seguridad constituye el elemento clave para que estas posibilidades puedan fructificar. Nada fuera de un inimaginable desastre impedirá que nuestra dependencia respecto de la Tecnología de la Información aumente a lo largo de los próximos años.

Así las cosas, ofrecer seguridad al ciberespacio constituye hoy un importante desafío que requiere el concurso de todos los agentes públicos y privados con responsabilidades en el sector.

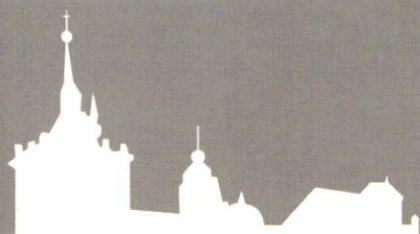
Sin perjuicio de aquellas otras contribuciones que se nos puedan demandar, nuestro papel resulta clave en la prevención de la utilización criminal de las posibilidades que la Sociedad de la Información ofrece y en la represión de los sujetos que abusarán de éstas. Asimismo, los sistemas de alerta temprana y los programas de gestión de crisis presentan ámbitos donde el beneficio de la colaboración del Cuerpo Nacional de Policía resultará muy importante.

Por último, la generación de una Conciencia de Seguridad en la Era de la Información constituye una estrategia de una utilidad y eficacia mayúscula. En ese sentido, confío que este seminario, en cuya concepción se refleja la importancia otorgada a los agentes públicos y privados, académicos y prácticos, nacionales e internacionales, refleje nuestro hondo interés por estos temas y nuestro convencimiento de que la seguridad de la Sociedad de la Información se apoya en la permanente disposición a responder a los cambiantes desafíos de la realidad, a las dinámicas demandas ciudadanas y a las estimulantes propuestas de los especialistas.



**PRIMER PANEL**

**LA SOCIEDAD DE LA INFORMACIÓN Y  
MARCO JURÍDICO**



# REDES Y SOCIEDAD DE LA INFORMACIÓN

**Félix Requena Santos**  
**Catedrático de Sociología de la Universidad de**  
**Santiago de Compostela**

Se definen las características y la estructura de la Sociedad de la Información. Se analizan las incidencias de las tecnologías de la información, la formación de las redes telemáticas, así como la revolución de las redes sociales y su significado en las vidas de las personas. Desde el punto de vista de la seguridad, son interesantes los aspectos vulnerables de la Sociedad de la Información, así como los de las redes y cómo éstos afectan a la vida cotidiana. Es importante prestar atención al proceso de globalización derivado e influenciado por la Sociedad de la Información. Estos dos procesos combinados generan un conjunto importante de peligros y situaciones críticas, como es el caso de la generación de los procesos de desigualdad y sus consecuencias: las redes terroristas.

21

## **CARACTERÍSTICAS, SIGNIFICADO Y ESTRUCTURA DE LA SOCIEDAD DE LA INFORMACIÓN**

### **Nuevas tecnologías: ordenadores y redes telemáticas**

Las redes abarcan todos los ámbitos de nuestra vida. Qué posición ocupamos, cómo trabajamos, dónde podemos ir, con quién nos relacionamos, cómo vivimos, es decir: afectan a lo que somos. Somos parte de las redes en las que estamos insertados. Esta dimensión reticular no es nueva, ni reciente en la historia de nuestras vidas, sin embargo se ha visto aumentada gracias a las tecnologías de la información, que han originado la sociedad de la información. La sociedad de la información no sería nada sin las redes: las redes tecnológicas, y las redes sociales que éstas originan.

La Sociedad de la Información se puede definir cómo aquella que usa de forma intensiva y extensiva las tecnologías de la información. Estas tecnologías se apoyan en dos componentes fundamentales: los ordenadores

y las redes. El uso masivo de los primeros y la extensión de las segundas han configurado un nuevo tipo de sociedad que abarca a todo el planeta, facilitando la capacidad de generar relaciones sociales a escala global. Estos nuevos modelos en la generación de relaciones son los que han puesto en marcha el gran proceso de cambio social que se ha llamado *proceso de globalización*.

La Sociedad de la Información ha puesto en funcionamiento el proceso de globalización, pero el proceso de globalización ha afianzado a su vez a la Sociedad de la Información. Con lo que estamos ante un doble proceso en el que cada uno reafirma y afianza al otro: globalización y Sociedad de la Información son difícilmente separables.

Del mismo modo que la máquina de vapor supuso el paso hacia la sociedad industrial, el ordenador ha sido el que ha generado la Sociedad de la Información. Es la sociedad donde el exponente principal es el tratamiento de la información y de las telecomunicaciones. El uso masivo de los ordenadores y de las redes telemáticas está afectando de forma directa e indirecta todos los ámbitos de la sociedad, porque la información que tenemos o que podemos tener genera y redefine nuestra realidad. Una realidad que se ve afectada en las nuevas formas de producir bienes y servicios; las relaciones internacionales; y, sobre todo, la forma en la que nos relacionamos con los demás. Pero, ante todo, se trata de una sociedad que está basada en el conocimiento que tenemos de la información. Por eso, también, se le ha llamado "sociedad del conocimiento".

22

Esta sociedad del conocimiento es una sociedad que se basa en la producción de servicios relacionados con la información, la formación y el conocimiento. No se trata de producir bienes, sino servicios. Es una sociedad postindustrial<sup>(1)</sup>. Estas sociedades se caracterizan por la gran dinamización social que impone la innovación de conocimientos. El conocimiento científico y tecnológico es el que vertebra estas sociedades. Es una sociedad basada en los conocimientos y la información, donde se produce información, se comercia con información y la posición social se mide por la cantidad de información que se posee. El actor principal en este tipo de sociedades es el técnico, el científico y el profesional innovador que es capaz de disponer y aportar nuevas ideas al manejo de la información.

El ordenador, y concretamente el ordenador personal multiplica la capacidad operativa de los individuos en el sistema social; capacidad que se ve multiplicada por las redes, lo que genera un cambio en la infraestructura de las relaciones de todo tipo: sociales, comerciales, institucionales, políticas, etc. Esta capacidad relacional se debe a que las redes no transportan materia, sino información, y lo hacen casi en tiempo real. Capacidad que es posible gracias una serie de cualidades que nunca se han dado con tanta fuerza antes de la revolución propiciada por las tecnologías de la información. Estas cualidades son:

---

1.- Bell, D. "El advenimiento de la sociedad postindustrial", Madrid, Alianza, 1991, p. 52.



**Instantaneidad:** la interacción y la comunicación se producen casi en tiempo real. La comunicación se puede establecer entre cualquier punto del planeta. El caso más útil y llamativo es el GPS (Global Position System). Esto permite la creación y funcionamiento de organizaciones con centros en puntos diversos del planeta. Es la base tecnológica de la globalización.

**Interactividad:** la comunicación es bidireccional, lo que permite tener una capacidad de respuesta constante.

**Interconexión:** la naturaleza digital de la información permite la existencia de protocolos de intercambio, con lo que se multiplica la capacidad de conexión entre diferentes elementos que constituyen las redes.

**Flexibilidad:** permite una gran funcionalidad para que estas tecnologías sean empleadas en una gran multitud de operaciones. Prácticamente, la única limitación que existe en su uso es la imaginación de los diseñadores (programadores).

**Convergencia:** desde el momento que toda la información es susceptible de ser digitalizada, estas tecnologías cuentan con la capacidad de integrar elementos que antes estaban dispersos en áreas diferentes, tales como imagen, sonidos, etc. Esto genera que estas tecnologías se puedan aplicar a una gran diversidad de operaciones.

**Capacidad de penetración:** el poder de procesamiento aumenta cada día; el precio se reduce, mientras que la capacidad de procesamiento es cada vez mayor.

El éxito del ordenador y de las tecnologías de la información se apoya, asimismo, en estos tres grandes procesos(2).

**Lingüístico:** está basado en la digitalización. Es decir, la capacidad de traducir percepción sensorial y símbolos humanos (expresión analógica) a códigos binarios simples basados en ceros (0) y unos (1) (expresión digital). La digitalización abre unas enormes posibilidades de operacionalización y computación, no sólo por su sencillez, sino por su universalización. Gracias a la digitalización se pueden traducir todo tipo de información (textos, imágenes, sonidos) a formato digital(3): ceros y unos; si y no; abierto y cerrado. El formato digital es el formato que "entienden" los microprocesadores.

2.- Bericat, E. "La Sociedad de la Información. Tecnología, Cultura, Sociedad", Revista Española de Investigaciones Sociológicas, 76, 1996, pp. 99-121.

3.- La unidad digital más simple (0,1) se conoce con el nombre de Bit (Binary digit). Un bit representa sólo dos valores. Dos bit, cuatro valores y ocho bits 256 posibles combinaciones de unos y ceros. Una unidad de medida muy utilizada en informática es el byte, que son grupos de ocho bits. Mediante combinaciones de bit y bytes se pueden representar todas las informaciones que se quiera, desde una biblioteca, hasta imagen y sonidos, etc. Una explicación sencilla sobre la combinación de unos y ceros en forma de bits y byte se puede encontrar en [www.ciberhabitat.gob.mx](http://www.ciberhabitat.gob.mx)

Esta sencillez tiene su fundamento en que los microprocesadores son circuitos electrónicos impresos en una pequeña porción de silicio (similar al vidrio) que procesa diminutos impulsos eléctricos. El microprocesador detecta cuando hay carga eléctrica y cuando no la hay, lo que equivale a que cuando hay carga eléctrica el dígito vale uno y cuando no la hay vale cero. Probablemente, este sea ahora el lenguaje universal: el lenguaje digital.

**Operativo:** el ordenador es sólo una máquina de computar. Es decir, cuenta códigos, ceros y unos. Sin embargo, su velocidad es tan alta que es capaz de procesar gran cantidad de información en microunidades de tiempo, lo que hace que la información se transmita casi en tiempo real. Desde que se inventó el primer chip en 1958, las velocidades de computación se han incrementado exponencialmente.

**Social:** con la aparición del ordenador personal en 1981, apareció la versión individual de los ordenadores, lo que ha generado la individualización del uso de la tecnología informática. Individualización que cada día se ve más potenciada gracias al uso de los ordenadores portátiles, cada vez más pequeños y potentes. Asimismo, el desarrollo de software cada vez más sencillo y amigable consigue que cada vez sean más personas las que usen este tipo de tecnologías en sus interacciones distantes con los otros.

## **Cambio social acelerado**

Esta sociedad del conocimiento se ha visto influida por los grandes cambios sociales que han tenido lugar a lo largo del siglo XX, y concretamente en la segunda mitad del siglo XX. Los avances de la medicina y los aumentos insospechados de la productividad, han logrado que la población pase de 1800 a finales del siglo XX, de algo más de 900 millones a 6 mil millones de personas. Pero si algo ha caracterizado al siglo XX ha sido el conocimiento. En el siglo XX se ha producido un gran avance en educación, que se ha universalizado; se han multiplicado el número de universidades y centros de investigación. Se han creado decenas de nuevas carreras y profesiones que antes no existían. Se ha progresado exponencialmente en sanidad y salud pública, lo que ha dado como lugar un aumento vertiginoso en la longevidad o la esperanza de vida. Todo ello gracias a que el conocimiento de la humanidad se ha multiplicado.

Estos cambios tan rápidos no hubieran tenido lugar si uno de los progresos no hubiese sido en de la transmisión de la información. Conocimiento, educación, investigación, salud, etc. se han multiplicado exponencialmente gracias a las posibilidades de difusión y a la facilidad de transmisión por medio de las tecnologías de la información y las telecomunicaciones. Las telecomunicaciones han sido el vehículo que ha facilitado el extenso e intenso cambio social y tecnológico que se ha producido a lo largo del siglo XX, y especialmente en la segunda mitad de ese siglo.



Los avances en las tecnologías globales de comunicación han sido los responsables. La comunicación vía satélite, capaz de transmitir imágenes en pocos segundos a lo largo de todo el planeta, ha hecho que la televisión se haya convertido en el medio de transmisión de contenidos mundial. Las redes globales de telefonía, con sus redes de fibra óptica. Internet, con el soporte de esa red telefónica mundial, ha sido capaz de transmitir mensajes de forma casi instantánea por todo el planeta. Si a esto le unimos el desarrollo y el abaratamiento de los medios de transportes intercontinentales, gracias a las redes de aviación civil y a la tecnología aeronáutica, entonces el planeta se ha hecho un lugar más pequeño, casi más familiar para todos.

## Globalización

Difícilmente se puede entender la Sociedad de la Información sin el proceso de globalización. La globalización, fundamentalmente la globalización económica, ha permitido la vinculación mundial de los mercados y de los sistemas de producción. Hoy las empresas producen sus productos sin la existencia de fronteras. Sin fronteras en el proceso productivo: se diseña en un país, se fabrica en otro, se ensambla en otros y el producto final se distribuye en otros diferentes, o en todos. Es lo que se llama la división internacional del trabajo. Pero lo mismo puede decirse de otros sistemas productivos más virtuales, como es el sistema financiero. Gracias a las tecnologías de las comunicaciones, e Internet, hoy no hay fronteras para los mercados de valores y los mercados financieros.

25

Se trata de la Economía Conectada. Los procesos económicos funcionan a lo largo de trayectorias complejas. La trayectoria que va desde lo nacional y lo local hasta lo internacional y lo global. De esta forma, conviven de forma conjunta procesos locales y regionales con los internacionales y mundiales. Es un proceso dual en el que confluyen diferentes niveles de empresas locales, regionales, nacionales e internacionales que se entrecruzan como consecuencia del hecho de moverse en un entorno de mercado difuso: no hay una limitación espacial clara y definida. Esta nueva dimensión de los mercados ha sido consecuencia del desarrollo de las nuevas tecnologías de la información. Con las redes de telecomunicaciones, la información traspasa las fronteras nacionales y se convierte en un bien difícilmente localizable en un espacio concreto.

Uno de los soportes materiales de la actual globalización es la nueva estructura empresarial, que está basada en la economía informacional. La economía informacional es internacional y global, nace en contextos nacionales y culturales muy diferentes que van desde una parte a otra del planeta. Su alcance es global e implica a todos los países y tiene un marco de referencia global. Este alcance planetario afecta a los actuales procesos empresariales que se basan fundamentalmente en procesos informacionales.

La información es la base del actual sistema productivo(4).

---

4.- Castells, M. "La era de la información: economía, sociedad y cultura", vol. 1. "La sociedad red", Madrid, Alianza, 1997, p. 179-180.



La clave ha sido la transformación en la organización de la producción y de los mercados. Esta transformación ha sido llamada de muchas formas por los científicos sociales: es lo que Piore y Sabel(5) han llamado la segunda ruptura industrial, o más bien la segunda revolución industrial; o lo que Daniel Bell(6) llamó la sociedad postindustrial, u otros han llamado simplemente globalización(7) o sociedad cosmopolita(8). Simplemente, se ha pasado de la cadena de producción de productos estandarizados a la producción flexible(9) de productos personalizados.

La producción flexible se apoya en las estructuras construidas con redes, lo que genera flujos de conocimiento. Estas estructuras reticulares permiten a las empresas dos cuestiones fundamentales: tener control e información casi instantánea de la propia empresa y su sistema de producción; y, al mismo tiempo, tener información sobre los requerimientos y las demandas del mercado(10). De esta forma, la propia organización de la empresa se hace sensible a la estructura y necesidades del mercado. Las empresas que se estructuran en forma de redes las hacen mucho más competitivas porque tienen en cuenta, con más rapidez y precisión, los flujos de información que les afectan.

Pero el verdadero poder globalizador de la tecnología de la información es la conectividad. La conectividad es la fuerza de la sociedad de la información. La conectividad genera una especie de "círculo virtuoso". La conectividad genera velocidad: cuanto más conectados estamos, más rápido podemos hacer las cosas. De este modo, se multiplican los aspectos intangibles de lo que podemos hacer en nuestro trabajo (como es el conocimiento), y las relaciones que podemos llegar a tener. Estos aspectos intangibles no tienen masa, por lo que circulan a gran velocidad a través de las líneas de conexión. Lo que hace que podamos tomarlos y enviarlos a grandes distancias y en muy poco tiempo. Velocidad, intangibilidad y conectividad se refuerzan mutuamente. Esta es una de las claves con la que las redes, basadas en las tecnologías de la información, están construyendo un mundo global. Un mundo que cada vez se hace más pequeño y más cercano.

5.- Piore, M. y Sabel, Ch. F. "La segunda ruptura industrial", Madrid, Alianza, 1990.

6.- Bell, D. "El Advenimiento de la sociedad postindustrial", Madrid, Alianza, 1991.

7.- Beck, U. "¿Qué es la globalización? Falacias del globalismo, respuestas a la globalización", Barcelona, Paidós, 1998.

8.- Beck, U. "The cosmopolitan perspective: sociology of the second age of modernity", British Journal of Sociology, 51, 2000, pp. 79-105.

9.- Coriat, B. "El taller y el robot. Ensayos sobre fordismo y la producción en masa en la era electrónica", Madrid, Siglo XXI, 1993.

10.- Esta es una de las claves del éxito de Zara, empresa española de confección. Gracias a las redes informáticas que ha construido entre sus más de 1500 tiendas repartidas por todo el mundo y su centro de producción en Arteixo (Galicia), ha logrado tener información sobre la demanda de sus productos, diseño, producción, y distribución de forma que cada 15 días es capaz de implantar en sus tiendas de todo el mundo los nuevos diseños que sus clientes van demandando. De esta forma, Zara renueva sus productos dos veces al mes. Todo un record que no hubiera sido posible sin las redes basadas en las tecnologías de la información. La clave del éxito está en la capacidad de obtener y procesar toda la información sobre los gustos de sus clientes de forma casi instantánea, lo que permite identificar las oportunidades de mercado, coordinar diferentes unidades de diseño y producción, y poner en marcha la distribución. La información se convierte así en uno de los recursos estratégicos más importantes que tienen hoy día las empresas.

## INCIDENCIA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

Las incidencias de las tecnologías derivadas de la Sociedad de la Información son tan numerosas como variadas, de forma que es difícil realizar un recuento de todas ellas. Sin embargo, comentaremos las principales y a las que las cuestiones de seguridad afectan con mayor premura. Sin embargo más importante que las tecnologías de la información lo que verdaderamente ha cambiado el mundo ha sido la potencialidad que las tecnologías de la información le ha permitido a la configuración de red. Las redes son las que verdaderamente están cambiando la estructura de muchas instituciones sociales. Las políticas nacionales, el funcionamiento de las empresas, no tienen sentido de una forma aislada, sino que su actuación tiene siempre que estar coordinada e interrelacionada con las instituciones con las que se nutre y a las que sirve.

El organigrama en el que se apoyan las instituciones flexibles de la Sociedad de la Información, no es un organigrama jerárquico sino uno reticular, donde los flujos de información sean lo más rápidos posibles. Las organizaciones necesitan que su personal realice tareas con un contenido más responsable en unos organigramas prácticamente sin escalones. Todo ello implica, entre otras cuestiones, saber trabajar en interrelación con las demás profesiones de la organización: comerciales, juristas, ingenieros, responsables de marketing, etc.; reunidos en torno a un grupo de proyectos, de células pluridisciplinarias o círculos de calidad etc.: trabajar en equipo. La Sociedad de la Información ha puesto los medios para trabajar en forma de red. Hoy cualquier organización que quiera obtener resultados necesita de una visión reticular de los problemas. Para ello ha de trabajar en grupos interdisciplinarios, donde cada uno sea capaz de aportar un aspecto diferente pero valioso de la realidad objeto de interés.

27

En la era de Internet es necesario saber encontrar la información. Hay que comprender, situar, poner en perspectiva. Por ello, el que puede aprender a aprender está en condiciones de ser flexible y de cambiar con su empresa sin tener que abandonarla cuando la empresa necesite cambiar. Otra consecuencia importante ha sido la multiplicación de servicios que ha ofrecido la Sociedad de la Información, sin embargo muchos de ellos no se desarrollan plenamente debido a los problemas de seguridad que todavía plantea la red Internet. Tal es el caso del comercio electrónico o, a nivel oficial, la administración pública a través de Internet. Sin duda, los sistemas de seguridad han avanzado mucho y cada día son más seguros: sistemas de encriptación, firma electrónica, servidores seguros, etc. hacen que se puedan realizar compras por la red, se pueda presentar la declaración de la renta o presentar un parte de accidente de trabajo por Internet. Sin embargo, estos sistemas constantemente están siendo violentados: virus, puertas traseras, robo de claves, asalto a oficinas gubernamentales, hacen que la confianza general no sea total.

El principal problema que tiene hoy día la seguridad en la red Internet es la confianza plena de los usuarios. No vale que Internet sea



segura, además de serlo tiene que parecerlo; tenemos que confiar en su seguridad. Si Internet nos parece segura, independientemente de que lo sea o no en su totalidad, entonces usaremos el e-comercio, la e-administración. La confianza determina la capacidad de definición de la situación que tenemos para utilizar un medio.

Por tanto tampoco conviene sobredimensionar algunas de las incidencias de las tecnologías disponibles en la Sociedad de la Información. Un caso bastante claro es el del teletrabajo. El hecho de trabajar desde casa, sin tener que ir a la oficina parecía que iba a ser la situación normal en la Sociedad de la Información, sin embargo esto no es así. En Estados Unidos, que es el país tecnológicamente más avanzado, sólo el 6,5% de la población trabajadora trabaja en casa, de esta cantidad sólo la mitad usa el ordenador, el resto usa sólo teléfono, papel y lápiz(11). En España (en 1999) este porcentaje se reduce al 2% de la población trabajadora, pero la media europea tampoco es muy alta: se sitúa en el 4%. El caso más significativo es el de Finlandia que alcanza el 10%(12).

### **SIGNIFICADO DE LAS REDES EN LA VIDA DE LAS PERSONAS**

28

Pero el uso de las tecnologías de la información no está restringido únicamente al mundo empresarial, sino que involucra a todas las actividades humanas que podamos imaginar. Es decir, afecta a toda la sociedad. Los ordenadores y las redes de telecomunicaciones se encuentran prácticamente en todas las áreas de la vida humana. Afectan a todas las áreas del gobierno, controlan el tráfico y las comunicaciones dentro de las grandes ciudades, y entre las ciudades y poblaciones de todo el mundo. Difícilmente quedan ya hogares donde no haya algún aparato que no tenga un microchip que controle su funcionamiento o que para funcionar haya dependido o dependa de alguna red telemática.

De este modo, los elementos que conforman y materializan la Sociedad de la Información han ido logrando poco a poco un proceso de cambio en nuestras mentes y en nuestras formas de percibir el mundo. Es decir, se ha producido un cambio cultural. Este cambio se debe principalmente a las posibilidades del uso de la información digitalizada en nuestras vidas. La palabra digital, en sí misma, se ha convertido en sinónimo de modernidad: si es digital es moderno, es mejor que analógico. Surge la dicotomía entre electrónico y mecánico. Electrónico y digital significa rápido, instantáneo; mientras que lo mecánico significa lento, secuencial.

Uno es sinónimo de inmediatez, el otro de lentitud.

El impacto de las tecnologías de la información ha sido tan grande y se ha extendido por tantos lugares, que hoy sería impensable la sociedad sin las tecnologías de la información. Sin embargo, su uso está reducido a

11.- Mokhtarian, P. "Telecommuting in the United States: letting our fingers do the commuting", Telecommuting Review: the Gordon Report, 9-5 (1992), p. 12.

12.- Sáez, E. "¿Cuántos son? ¿Cuántos somos?". Deteletrabajo.com, nº 8, 21 febrero de 2001.



un número relativamente pequeño de habitantes en el planeta. Según diversas fuentes, de Naciones Unidas y de usuarios de Internet, no más de un tercio de los habitantes del planeta nunca ha usado el teléfono, sólo cerca del 9% de la población mundial tiene acceso a un ordenador, el 3% tiene teléfono móvil, y aproximadamente el 7% tiene acceso a Internet.

Si la distribución de las tecnologías de la información tiene esta distribución tan desigual en el planeta, ¿cómo es posible que tengan una incidencia tan grande? La respuesta es que la mayoría de los ordenadores, y las redes telemáticas, así como el resto de las infraestructuras se concentran en los países más desarrollados y en los polos de mayor modernidad de los países intermedios y pobres, con lo que acaparan las principales funciones políticas y económicas de la sociedad(13). Sin embargo, las tecnologías de la información, gracias a su flexibilidad y a su capacidad de conexión y de penetración han llegado a casi todo los puntos del planeta, aunque su control sea accesible de forma muy desigual.

En España, los datos relativos al uso de las tecnologías de la información tienen el perfil de los países desarrollados occidentales. Según datos de la Asociación de Usuarios de Internet (AUI), a finales del 2001 un tercio (33,3%) de los españoles usa el ordenador y en marzo del 2003 algo más de un cuarto (25,5%) de los españoles son usuarios de Internet. La gran mayoría de ellos (en marzo 2003) usa Internet en el trabajo (31,2%), en casa (61,1%) o en la Universidad (14,1%). Estos datos tienen mucho más sentido si se presta atención a su evolución. Por ejemplo, en marzo de 1996 era usuario de Internet el 0,7% de la población española, frente al 25,5% actual (desde esa fecha hasta hoy, 7 años, se ha multiplicado por 37 veces). También tiene sentido ver la variación en la distribución del lugar desde donde se accede a Internet: en noviembre de 1996, el principal punto de acceso era el trabajo (46,4%) seguido de la Universidad (22,7%). Sin embargo, hoy marzo de 2003, el principal punto de acceso es en casa (61,1%) seguido por el trabajo (31,2%) y la Universidad (14,1%). Estos datos ponen de manifiesto el rápido crecimiento del acceso a las redes informáticas, y al cambio cualitativo que han supuesto en nuestras vidas, tal como indica el hecho de que hoy se use más Internet desde casa que desde el trabajo. Esto le da un componente mucho más personal, y no exclusivamente laboral que tiene para los españoles el uso de Internet.

Otro dato importante respecto a la implantación de Internet en las vidas de los españoles es la evolución en el perfil de sus usuarios. A finales de 1996 (nov. 1996) los usuarios de Internet eran un 75,4% varones y un 24,6% mujeres, sin embargo, hoy (marzo 2003) son el 59,5% varones y el 40,5% mujeres. En 7 años se ha pasado de una diferencia de 50,8 puntos porcentuales a 19 puntos porcentuales. Lo mismo ocurre con la edad, mientras que en noviembre de 1996 el principal grupo que usaba Internet era el de 25 a 34 años de edad, hoy (marzo 2003) este grupo sólo es del

13.- Castells, M. "La galaxia Internet", Barcelona, Random House Mondadori (debolsillo), 2001.

29,8% encontrándose los demás grupos repartidos de forma mucho más homogénea(14).

Por regiones, el uso de Internet, se concentra en Cataluña y Madrid o País Vasco, con un 27,1 y un 27 por ciento de su población, respectivamente. Teniendo una implantación más escasa en comunidades como Castilla-La Mancha con un 14,6%, o Extremadura con un 15,6% de su población que usa Internet.

España se muestra así como un país donde las tecnologías de la información le hacen funcionar como un país occidental donde se concentra el uso de las tecnologías de la información. Aunque, sin duda es evidente la diferencia con los primeros puestos en el uso de Internet en el mundo. Según datos de la AUI para abril de 2002 en España el 22,7% de la población era usuario de Internet frente al 67,8% de Suecia, 62,9% de Dinamarca, el 60,9% de Holanda o el 58,9% de Estados Unidos. Una vez más los países nórdicos se evidencian como unos de los más avanzados.

## **FUTURO DE LA SOCIEDAD DE LA INFORMACIÓN. PUNTOS MÁS VULNERABLES**

### **Sociedad del riesgo global**

30

La Sociedad de la Información es una sociedad global. Por tanto los riesgos son globales: no terminan ni empiezan en ningún lugar concreto, o al menos es muy difícil concretarlo. Esto nos lleva a pensar en el argumento de Ulrich Beck(15) sobre la sociedad del riesgo, y concretamente sobre la sociedad del riesgo global.

En este tipo de sociedad se producen amenazas y vulnerabilidades del sistema a nivel global. Las amenazas no son ya amenazas a un sistema concreto, sino que la vulnerabilidad viene derivada de la complejidad de interrelación que presentan todos los sistemas entendidos como un conjunto que interactúa en forma de una inmensa red. Sin embargo, se puede establecer una tipología de amenazas globales.

1. Conflictos motivados por la riqueza. Son los derivados por el exceso de aplicación desmesurada de tecnología. Es decir, destrucción ecológica, tales como la destrucción de la capa de ozono, efecto invernadero, riesgos impredecibles derivados del uso de la tecnología nuclear, de la manipulación genética de plantas y seres humanos.

2. Riesgos relacionados con la pobreza. Existe una estrecha relación entre la pobreza y la destrucción ambiental. Evaluar estos riesgos supone un análisis integrado de la vivienda, la alimentación, los recursos de todo tipo (genéticos, energéticos, industriales, etc.) estos riesgos inciden en la población humana y se manifiestan en múltiples y diversas formas de violencia.

---

14.- Para los datos de acceso a las redes y el uso de ordenadores puede consultarse la página web de la Asociación de Usuarios de Internet. [www.aui.es](http://www.aui.es)

15.- Beck, U. "La sociedad del riesgo global", Madrid, Siglo XXI, 2002; y "La sociedad del riesgo", Barcelona, Paidós, 1999.



3. Armas de destrucción masiva sean del tipo que sean, químicas, nucleares, biológicas, etc. son la nueva amenaza que justifican intervención armada (guerra de Irak). El peligro de destrucción que suponen ha escapado a toda estructura de control y seguridad. Junto a la amenaza de conflicto militar entre Estados, está ahora la amenaza (convertida en realidad) del fundamentalismo de diverso tipo (nacionalista, fundamentalista, etc.) y el terrorismo que entran en las redes de tráfico de este tipo de armas.

En la sociedad del riesgo global las amenazas son globales. Los peligros actuales están eliminando los cimientos convencionales del cálculo de la seguridad. Los daños pierden sus límites espacio-temporales y se convierten en peligros globales y duraderos(16). En este estado de la situación las amenazas y riesgos no son nada en sí mismos sino que están vinculados con conflictos étnicos, nacionales, recursos que se consideran agotados, etc. El fin de la confrontación Este-Oeste, ha supuesto un resurgimiento de cientos de pequeñas confrontaciones variopintas y dispersas pero vinculadas entre sí en una peligrosa red de difícil desmantelamiento.

Sin embargo, en una sociedad como la de la Información, la ciencia parece ser la fuente para el control de todo. Pero hay circunstancias que no pueden prever su malfuncionamiento hasta que éste no se produce, y entonces es cuando pueden actuar los sistemas de seguridad. Hasta entonces los sistemas de seguridad serán simplemente "sistemas supuestos de seguridad". Por ejemplo, hasta que no explote una central nuclear no se comprueba la eficacia del sistema de seguridad, lo mismo ocurre con la investigación genética, o las redes informáticas. Bien es verdad que existe mucha investigación en seguridad de sistemas críticos, pero por mucha investigación que se realice siempre se estará a expensas de los "círculos de seguridad", es decir, cómo funcionará el sistema de seguridad previsto cuando se produzca la catástrofe. Se produce el círculo: catástrofe-seguridad-catástrofe-seguridad. Aunque bien es verdad que tras cada catástrofe mejoran los sistemas de seguridad.

Esto nos lleva a un replanteamiento de seguridad. En la era de riesgos múltiples en la que vivimos, la única forma de seguridad es repensar todo lo que conocemos desde el planteamiento de la interrelación. Del mismo modo que en las redes todos los nodos terminan afectándose mutuamente, en la actualidad, las situaciones peligrosas están afectadas por causas interrelacionadas. En el mundo actual la verdadera seguridad es la que viene de pensar y vigilar en todos los frentes lo más simultáneamente posible.

Estos tipos de riesgos se pueden resumir en uno principal, que a su vez es muy antiguo: los conflictos derivados de la desigualdad. La desigualdad es el principal problema "ambiental" del planeta. La desigualdad social basada en la desigualdad del conocimiento, de la ciencia, de la comunicación y de la información está generando una dependencia del conoci-

16.- Beck, U. "La sociedad del riesgo global", cit. p. 57.



miento. La distribución de la información y las oportunidades de acceso a las redes de información no sólo imponen y posibilitan la reorganización de la producción y la creación de riqueza, sino que la falta de acceso a ellas puede conducir a una radicalización de la desigualdad social lo que puede llevar a un nuevo destino a los "excluidos", y este destino basado en la necesidad puede llevar a escapar de todas las redes de seguridad que se puedan construir o diseñar. Este es uno de los verdaderos peligros y vulnerabilidades de la nueva Sociedad de la Información.

### Procesos de desigualdad

Uno de los puntos más controvertidos a los que está dando lugar la Sociedad de la Información es a la sensibilidad ante los procesos de desigualdad social. En este punto, Sociedad de la Información y globalización actúan como sinónimos. La pobreza es una de las cuestiones que más tenemos que tener presente, porque la pobreza en la Sociedad de la Información no es igual que la pobreza en los anteriores tipos de sociedad. En las sociedades anteriores a la Sociedad de la Información las situaciones de pobreza no podían ser comparadas con el resto de la población no pobre. Sin embargo, hoy con los medios de comunicación de masas (MCM) al alcance de todos, las masas están en condiciones de medir su posición relativa respecto al resto de la población que posee una abundancia de bienes. Esta situación de concienciación de la pobreza produce una situación de cambio cualitativo en los niveles de pobreza. Situación que supone un apoyo para la movilización de los desamparados. Un ejemplo bien sencillo de esta situación son los movimientos migratorios globales que se están produciendo en el mundo globalizado de la Sociedad de la Información. En África hay veinte millones de personas que están dispuestas a pasar a Europa, veinte millones que han tomado la decisión y si no cruzan el estrecho ahora mismo es porque no pueden, lo que no significa que no vayan a intentarlo en el futuro inmediato. Es la movilización de la pobreza. Pero lo mismo se puede decir de Hispanoamérica o de los países del Este de Europa.

La Sociedad de la Información ha concentrado sus recursos, financieros y materiales, en las zonas centrales del mundo. Pero los MCM muestran esa concentración de recursos al resto del mundo, gritándoles lo que hay en él. Consecuencia, se produce una movilización hacia las grandes ciudades de los países occidentales, con lo que se generan bolsas de pobreza nutridas con inmigrantes en las zonas centrales de los principales países de occidente. De modo que para encontrar pobreza no hay que ir a África, basta con salir a las calles de Madrid o de cualquier ciudad española. Esto genera una gran cantidad de tensión que, a su vez, es la fuente de una gran cantidad de conflictos.

La Sociedad de la Información ha facilitado el proceso de dispersión y diversificación de las empresas de todo el mundo, sin embargo, esto significa un mayor crecimiento de las empresas del primer mundo. Por ejemplo, los países de la UE se han enriquecido entre un 50 y un 70% en los últimos 20 años, sin embargo, la UE tiene ahora 20 millones de para-

dos, 50 millones de pobres y 5 millones de personas sin techo. El 96% del plus de riqueza generada en estos últimos 20 años ha ido a parar al 10% de población más acomodada. Esta es la situación de la nueva desigualdad social, que en la actualidad es el principal núcleo del conflicto social moderno como lo llama Darhendorf(17).

Un ejemplo de la importancia de la sensibilidad ante los procesos de desigualdad en la Sociedad de la Información son los movimientos anti-globalización. Estos movimientos difícilmente se podrían dar sin una gran facilidad para contactar (medios de comunicación baratos: Internet, e-mail) y para movilizarse (medios de transporte baratos: venta de pasajes de avión por Internet). Los movimientos antiglobalización es el grito desesperado del incremento de la desigualdad, la pobreza y la exclusión social. Más de dos terceras partes de la humanidad no se benefician del nuevo modelo de crecimiento económico(18), Internet llega a menos del 8% de la población mundial. La solución es hacer un esfuerzo por la democratización de la globalización. Es decir, la inversión y la redistribución en los países subdesarrollados y en vías de desarrollo. Sin duda, una forma de disminuir los flujos de las migraciones de la pobreza es invertir en los países de origen. Reducir la inmigración marroquí invirtiendo en Marruecos.

Lo que significó Seattle y continuó con las sucesivas reuniones del G7, el FMI y la OMC es "el fin de la ilusión neoliberal de un planeta autogestionado por los mercados para el beneficio de los más fuertes, de los más listos y, también, de los más pillos"(19). La sociedad civil global está haciéndose oír, y lo está haciendo a través de los medios que pone a su alcance la Sociedad de la Información.

El proceso de globalización se ha visto reforzado por las comunidades on-line. Se trata de comunidades semejantes a las comunidades contraculturales de los 60 pero surgidos de la necesidad de sentimiento comunitario ante el fracaso de los experimentos contraculturales en el mundo físico(20). Este proceso da lugar a comunidades tan diversas como la propia sociedad (ecologistas, extrema derecha, etc).

### **Delincuencia derivada de la desigualdad**

Hay que ser muy sensible a los procesos de desigualdad porque éstos pueden, con mucha facilidad, llegar a convertirse en puntos de delincuencia y conflicto social. Para que exista paz social es necesario cubrir unos mínimos de necesidades vitales (alimento, vestido, vivienda, educación, sanidad, etc.). Cuando estas necesidades no se pueden cubrir por mecanismos legales se cubren con los ilegales. Este proceso es el que hace que núcleos de inmigrantes se conviertan con facilidad en focos de delincuencia.

17.- Darhendorf, R. "El conflicto social moderno", Madrid, Mondadori, 1990.

18.- Castells, M. "Seattle y el cinismo neoliberal", El PAIS, 3 enero de 2000.

19.- Ibid.

20.- Castells, M. "La galaxia Internet", cit. p. 79.



La Sociedad de la Información también facilita un tipo de delincuencia propia del uso de los poderosos medios que facilita la tecnología de la información. Cuando esta tecnología de la información se usa en procesos delictivos, más o menos organizados, es cuando hay que prestar atención a los procesos de seguridad formalizados.

La combinación entre globalización, Sociedad de la Información, y los procesos de desigualdad generado por ambas han dado lugar a situaciones de alto riesgo o peligros globales. El caso más notorio ha sido el atentado a las torres gemelas de Nueva York el 11 de septiembre de 2001.

Este o estos atentados abren una nueva situación y una nueva perspectiva en los sistemas de seguridad de los países desarrollados: las redes terroristas. En estas redes no existe un objetivo ni un sujeto claro y definido al que hay que localizar y detener. En el caso de las torres gemelas se trata de las redes fundamentalistas islámicas terroristas contra las instituciones políticas y económicas de los países ricos y poderosos (Estados Unidos y Europa Occidental). Estas redes surgen como rechazo a la marginación islámica y el sentimiento de rechazo a su cultura y religión por parte de los poderes occidentales. Esta oposición se concreta en la oposición a la existencia de Israel, y continúa candente en el constante enfrentamiento palestino-israelí. Pero las redes terroristas no son sólo islámicas. Las redes terroristas son diversas, dispersas y heterogéneas. Cuentan con orígenes diversos, incluidos sectores de la economía criminal, sectores de los desmantelados servicios secretos de los países del Este europeo(21), etc.

34

Después de estos atentados hay que prestar mucha más atención a lo que es el soporte de la Sociedad de la Información: la información. Precisamente lo que ha fallado en los servicios de seguridad, en este caso norteamericano, han sido los servicios de información. Lo que lleva a repensar los ejércitos que tenemos y, sobre todo, que necesitamos. El 11 de septiembre fue un manifiesto fracaso de los servicios de información, de los servicios secretos del mundo desarrollado.

Pero la situación no ha cambiado desde entonces. Las dos grandes intervenciones en defensa de la seguridad occidental que han sido la guerra en Afganistán contra la red de Bin Laden, o la guerra de Irak contra un régimen de descontrol de armamento, han fallado en uno de sus principales objetivos (aunque no en el hecho simbólico de capacidad de reacción ante los ataques terroristas) el eliminar a lo que se supone son los dos nodos centrales de sus respectivas redes o al menos de dos núcleos importantes de la misma red. Ha fallado la información, la consecuencia es el paradero desconocido tanto de Bin Laden como de Sadam Hussein(\*).

21.- Una vez terminada la guerra fría, buena parte de los ex servicios secretos de aquellos países en los que se cayó el aparato para el que estaban pensados, han ido a formar parte de las mafias que están actuando en el resto de Europa y en España. Estos ex agentes han ido a engrosar este tipo de actividades por varias razones: conocen la actividad, conocen la tecnología para llevarla a cabo, de forma que la ponen al servicio del Estado o de cualquiera que quiera lucrarse con ella. Ver Campo Vidal, M. [www.uoc.es](http://www.uoc.es).



## LA SEGURIDAD DE LAS REDES Y SU EFECTO EN LA VIDA COTIDIANA

Desde el punto de la seguridad, las redes tienen una serie de cualidades funcionales que les hace ser tremendamente operativas para conseguir sus objetivos (en este caso delictivos): Son 1) dispersas, 2) ubicuas, 3) heterogéneas.

1. La dispersión de las redes hace que sean difíciles de localizar en un punto concreto, lo que les permite luchar en varios frentes. Esto significa que las fuerzas de seguridad tienen una gran dificultad para situar su actuación. Por lo que surge cada día más la necesidad de la cooperación de las fuerzas de seguridad de varios territorios (colaboración internacional).

2. Ubicuidad. Permite a las redes la actuación simultánea en diferentes lugares al mismo tiempo. Esta característica refuerza el objetivo logrado con la dispersión, lo que supone mayores problemas de seguridad para su control.

3. Heterogeneidad. Esta es la verdadera potencia de las redes sociales, y las redes terroristas o criminales son redes sociales. La heterogeneidad hace que las redes sean más funcionales, abarquen todos o una gran mayoría de los aspectos de los que tiene que cubrir. Por ejemplo, las redes interdisciplinarias de científicos producen más que las redes formadas por científicos de una sola disciplina. Cuando esta heterogeneidad se plasma en redes criminales, éstas se hacen más difíciles de controlar y de dismantelar porque cubren muchos más aspectos y matices de funcionamiento, de forma que es difícil para los sistemas de seguridad predecir todos sus niveles de actuación. Por este motivo, casi siempre sólo se puede ir por detrás de ellas.

La forma de actuación de las redes terroristas tiene cierta similitud con el funcionamiento de la tan temida la guerra de guerrillas que utiliza técnicas difícilmente manejables por los ejércitos organizados de una forma convencional.

Para luchar contra estas redes lo primero que es necesario saber es: contra quién se lucha; cómo se supone que sea su actuación. Y sólo entendiendo este tipo de estructura reticular se puede llegar a su neutralización. Es decir, desde una pluralidad de valores e intereses. No estamos ante un grupo definido en términos precisos es una lucha contra un organismo que tiene vida propia.

Las redes terroristas combinan varias potencialidades: incluyen a sectores desfavorecidos de la sociedad, que están dispuestos a casi todo porque nada tienen y nada pierden; incluyen sectores de la sociedad especializados en organización criminal, tráfico de drogas, armas (nucleares), pueden encontrar tácticas de colaboración redes fundamentalistas (religiosas, nacionalistas, separatistas, etc.). Estos son los dos bloques de poder que han sustituido a los antiguos de la guerra fría. Son, por un lado, el bloque de los

países occidentales y orientales que participan del sistema económico y tecnológico avanzado, y por otro el bloque de las redes terroristas formadas por fundamentalistas, algunos gobiernos, y con alianzas tácticas con otras redes terroristas y con una simpatía difusa en los ciudadanos de algunos países pobres(22). La Sociedad de la Información ha generado sus propias células cancerígenas, que al igual que esta enfermedad moderna nunca se sabe con precisión donde va a afectar ni por donde se va a extender.

También existen otros peligros originados por la Sociedad de la Información: son la delincuencia común que usa la potencialidad de las redes y la tecnología de la Sociedad de la Información; delitos informáticos; invasión de sistemas de privacidad; intrusión de virus informáticos en la red; asalto a redes de seguridad privados o gubernamentales, etc.

La ventaja de Internet ha supuesto también su inconveniente (su vulnerabilidad). La base de la potencialidad y del desarrollo de Internet ha sido precisamente que sus códigos estaban abiertos a todos los que quisieran mejorarlos. Esto ha supuesto una ventaja y un inconveniente. La ventaja ha sido que cualquiera que tuviera los conocimientos necesarios podía acceder y mejorar el sistema (hackers). Su inconveniente es, asimismo, que cualquiera que sepa y tenga malas intenciones puede vulnerar el sistema (crackers).

36

Este inconveniente es el que hace que surja la necesidad de proteger los sistemas "sensibles", es decir, aquellos que tienen información valiosa para ellos mismos o para terceros: bancos, ministerios y oficinas gubernamentales, policía, etc.

Asimismo, la vulnerabilidad del Estado ante los ciberataques se debe al surgimiento de un Estado red global surgido de la cooperación entre gobiernos de todo el mundo en un conjunto amplio de cuestiones, incluida la seguridad. La ampliación de esta red no sólo a otros Estados sino también a un número creciente de organizaciones, logra una especie de gobierno compartido. Sin embargo, en estas condiciones en las que la red es cada día más grande, compleja y heterogénea, la seguridad de uno de sus nodos (aunque sea muy importante) dependerá de la seguridad de la red en su conjunto, y lógicamente ésta no suele ser muy buena. Esto lleva a que los Estados distingan varios niveles de confianza y acceso según el socio de que se trate. Sólo los socios más dignos tienen acceso a las redes de los sistemas más estratégicos(23).

El desarrollo y, sobre todo, el abaratamiento de las tecnologías de la información ha dado lugar a la proliferación del "cibercrimen": delincuencia de guante blanco que utiliza los nuevos medios tecnológicos(24).

22.- Castells, M. "La guerra red", EL PAIS, 18 septiembre 2002.

23.- Castells, M. "La galaxia Internet", cit. p. 206.

24.- Existen multitud de ejemplos recientes de este tipo de delincuencia: red colombiana de falsificación de tarjetas para cajeros automáticos: se pone un dispositivo en los cajeros de España, se toman clandestinamente las claves de las tarjetas, se envía la información a Sudamérica donde se producen tarjetas falsas que se distribuyen otra vez en Europa.



Delincuencia que ve aumentada su capacidad de actuación cuando se organiza en forma de red. De ahí que no sólo sea importante diseñar nuevos sistemas de encriptación y de firma digital, sino de conseguir que los accesos a los sistemas protegidos no sean capaces de permitir el acceso vía una "puerta trasera" más vulnerable a las estructuras de red(25).

De todo lo expuesto se puede concluir con tres situaciones de vulnerabilidad que se pueden derivar de las redes en la Sociedad de la Información:

En primer lugar, se encuentra la situación de falta de confianza que conllevan los problemas de seguridad en las redes informáticas, lo que origina que éstas no logren plenamente toda la funcionalidad de la que es capaz su diseño.

En segundo lugar, nos encontramos con los problemas de seguridad derivados de los procesos de desigualdad social, lo que implica diferentes tipos de violencia, y a su vez a la necesidad de escapar a las redes de seguridad.

En tercer lugar, la Sociedad de la Información junto con el proceso de globalización y los procesos de desigualdad que éstos ha generado producen situaciones de alto riesgo, como es el caso de las redes terroristas las cuales, dada su alta heterogeneidad, tienen un gran poder de actuación. Estas redes están resultando ser uno de los elementos que hace más vulnerable el desarrollo de las sociedades actuales.

---

25.- Uno de los últimos virus conocidos hasta la fecha (7 de junio de 2.003), el BugBear, distribuido a través de los e-mails, es capaz de anular la protección antivirus, consigue no levantar sospechas porque no provoca funcionamiento anómalo en nuestro ordenador, sin embargo, el virus habrá abierto en nuestra máquina una "puerta trasera".

(\*) **Nota del editor:** en las fechas de celebración del Seminario, Sadan Hussein todavía no había sido detenido.



# **CIBERESPACIO: LIMITACIONES JURÍDICAS Y PROCESALES**

**Alberto Dorrego de Carlos**  
**Director General para la Modernización de**  
**la Administración de Justicia**

## **CONSIDERACIONES GENERALES**

La actual Sociedad de la Información, en cuanto tiene su base en la informática y en las nuevas tecnologías, no es completa y continúa siendo evolutiva, sometida a continuos y progresivos cambios a tenor de cada nuevo desarrollo tecnológico, como la digitalización o la creación de espacios virtuales, que producen asimismo sobresaltos en las previsiones legislativas y necesarias adecuaciones o modificaciones legales ante las nuevas situaciones o supuestos de hecho que se presentan con dichos avances tecnológicos.

El uso indebido del ordenador y de la tecnología informática se constituye en una amenaza global, y la seguridad de los modernos sistemas informáticos se ha constituido en una cuestión principal para la Sociedad de la Información de nuestros días, debiéndose tener presente que los cambios que estas nuevas tecnologías causan en la ley penal y procesal conciernen no sólo a los delitos tradicionalmente calificados como informáticos, sino a todo tipo de delitos.

Juristas y sociólogos llevan tiempo discutiendo el impacto social de la tecnología moderna. El entramado de redes informáticas traspasa fronteras territoriales, transportándonos a un mundo virtual con lo que estas nuevas tecnologías nos aportan beneficios y configuran un progreso social y económico, pero también dan lugar a conductas antisociales y delictivas, es lo que modernamente se denomina "Sociedad de Riesgos". Internet representa un espacio ideal para las conductas delictivas, debido a dos factores: la facilidad comisiva y las dificultades para su persecución. Bienes jurídicos como la intimidad, el patrimonio, la indemnidad sexual de la infancia, la

propiedad industrial, la propiedad intelectual o la confianza en la integridad de determinados documentos, son sólo algunos de los valores que pueden quedar frágilmente expuestos a un intenso menoscabo originado por conductas amparadas en el anonimato que ofrece la red.

La gran mayoría de la doctrina especialista o no en la materia, ha considerado que la criminalidad informática queda comprendida dentro de la compleja problemática propia de una "sociedad de riesgos", y necesitada de una regulación en ámbitos diferentes como la protección de los derechos de la personalidad y de la propiedad intelectual, una reforma del proceso penal para su adecuación y adaptación a estos nuevos medios comisivos del delito informático, y una legislación internacional para poder traspasar las barreras jurisdiccionales en la persecución y enjuiciamiento de los delitos que extienden sus efectos más allá de las fronteras del Estado en el que se ha llevado a cabo la acción. En definitiva, la Sociedad de la Información necesita de una legislación adecuada al modelo social y a las tecnologías involucradas. Las TIC requieren un marco legislativo particular, tanto para tipificar nuevas conductas delictivas como para encauzar su uso y desarrollo. Es una tarea compleja, que requiere de un profundo trabajo interdisciplinario para lograr una legislación que a la vez contemple las necesidades de la sociedad y las realidades de la tecnología.

40

Por otro lado, este nuevo panorama, jurídicamente exige que tanto las autoridades judiciales y el Ministerio Fiscal deban adaptarse a este tipo de investigaciones, para proteger los intereses y recursos de la sociedad, preservando al mismo tiempo los derechos y libertades de los ciudadanos, así como que las Fuerzas y Cuerpos de Seguridad del Estado deban también adaptarse para poder operar, necesitando obtener conocimientos sobre los nuevos métodos y técnicas de investigación.

En esta intervención, se tratará analizar someramente el actual marco jurídico de estos delitos derivados de las nuevas tecnologías, tanto en su vertiente sustantiva como procesal, haciéndose necesario referirnos por un lado, a la reciente Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, que entró en vigor en octubre de 2002, al Convenio de asistencia judicial en materia penal entre los Estados miembro de la U.E., cuya Declaración de Aplicación Provisional ha sido recientemente aprobada por el Senado; y por otro, al Convenio sobre la ciberdelincuencia, conocido también como Convenio sobre el cibercrimen, elaborado en el seno del Consejo de Europa, abierto a la firma en noviembre de 2001 en Budapest. Tampoco faltará una necesaria alusión a la regulación que se propone en el Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.



## MARCO JURÍDICO DE LOS DELITOS DERIVADOS DE LAS NUEVAS TECNOLOGÍAS.

### 1. Necesidad de intervención del Derecho Penal

Es conocida la polémica existente acerca de la necesidad o no de intervenir jurídicamente en la Red. Nuestra legislación actual, con el C.P. de 1995, ha iniciado una ampliación del ámbito de protección a través de la creación de nuevas tipicidades que pretenden la tutela de nuevos bienes jurídicos que han recibido la denominación de “difusos” o bien de bienes jurídicos supraindividuales. El derecho penal español basado en los principios de fragmentariedad, subsidiariedad y mínima intervención, según los cuales el ius puniendi estatal deberá ejercerse tan sólo ante las más graves vulneraciones de los intereses sociales más importantes y siempre que no existan formas de control social menos gravosas que el control penal, en algunos casos, ha retrocedido en su espacio de acción, descriminalizando algunas conductas punibles y en otros, ha creído conveniente la represión de nuevas conductas consideradas dañosas.

Es en este contexto donde debemos situar la criminalidad informática, y preguntarnos si el derecho penal está preparado para solucionar los conflictos que se producen en la red, o por el contrario, dejar en manos del derecho administrativo la resolución de conflictos que aquí se generan.

41

Puestos en la tesitura de tener que abogar por la intervención del derecho penal en esta nueva forma de criminalidad, aquél tiene serios obstáculos para facilitar su aplicación debido a las peculiares características de esta delincuencia informática, peculiaridad que viene dada tanto por el lugar en el que el delito se comete - el espacio donde va a producirse la conducta delictiva no es un espacio físico sino que es un espacio virtual, es lo que se denomina el ciberespacio-, por el medio que se utiliza para su comisión, así como por las características de sus autores (podríamos citar a los Hackers-aprovechan los fallos de los sistemas de seguridad-, y los Crackers o piratas informáticos que son aquellos que se cuelan en los sistemas informáticos produciendo serios destrozos, diferenciándose de aquéllos en la intencionalidad ).

### 2. Medidas legales previstas en el derecho penal

Buscar una definición de delito informático no es fácil, desde el momento en que actualmente la doctrina mayoritaria niega la noción de delito informático, entendida aquélla como una categoría jurídica con sustantividad propia. El delito informático tiene un significado puramente instrumental, con arreglo al cual, más que un delito informático existen tantos delitos informáticos como infracciones penales sean susceptibles de ser cometidas valiéndose de medios informáticos. Es por ello que la mayoría de los autores hablan de delincuencia informática o criminalidad informática.

El legislador del C.P. de 1995 optó por reaccionar frente a las conductas delictivas informáticas mediante lo que se denomina “tipos de equi-



valencia", es decir, redactar cláusulas que complementen a los tipos ya existentes, con la finalidad de corregir las insuficiencias que en su aplicación se han detectado. Así se introdujeron en las diferentes descripciones típicas el nuevo medio comisivo utilizado, es decir, el ordenador, el sistema informático, que se constituye básicamente como el medio a través del cual el autor puede acometer de una manera más fácil un hecho delictivo, al contrario que las legislaciones de otros países como Holanda o el Reino Unido, que recogen de forma especial sus descripciones relativas a este tipo de delitos.

En Derecho Penal español no existe un delito informático. Hay una realidad criminal compleja que se encuentra vinculada a las nuevas tecnologías de la información, y que es imposible reconducir a un único tipo legal. El Código Penal de 1995 contiene distintas referencias a lo informático; por otra parte, siempre que el legislador, al redactar un tipo penal, no excluya expresamente el medio de comisión informático, debe entenderse que el mismo está incluido.

Las parcelas que sufren mayores efectos de los delitos a través de los medios informáticos son:

1º) Los atentados contra intereses de contenido económico, particularmente a través de los siguientes preceptos:

42

Artículo 239 in fine (utilización de tarjetas electromagnéticas en relación con el robo con fuerza)

Artículo 248.2 (estafa informática)

Artículo 256 (intrusismo informático)

Artículo 264.2 (sabotaje informático)

Artículos 278, 279, 280 (espionaje informático)

2º) Las falsedades documentales contenidas en los artículos 390 y siguientes, que partiendo del nuevo concepto de documento contenido en el art.26 del C.P. comprende también el documento electrónico.

3º) Los atentados contra la intimidad (con referencias específicas a "lo informático" en el art.197 del C.P.).

4º) Delitos contra la propiedad intelectual (art.270)

5º) Difusión y exhibición de material pornográfico a menores (art.186)

6º) Pornografía Infantil (art.189)

7º) Difusión de mensajes injuriosos o calumniosos (art.211)

8º) Publicidad engañosa.

### **3. Regulación del Anteproyecto de ley orgánica por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal**

En esta materia de la delincuencia informática, el legislador ha sido consciente que la regulación establecida hasta ahora se ha revelado en algunos campos insuficientes, es decir, la inclusión en el tipo de términos como “manipulación informática”, “redes, soportes o sistemas informáticos”, etc., se han quedado cortas para conseguir una correcta tipificación de las conductas ilícitas que pueden cometerse en y a través de internet.

Así en dicho Anteproyecto el legislador dice en la Exposición de Motivos lo siguiente: “era preciso adaptar sus disposiciones a las nuevas necesidades surgidas tanto de la experiencia acumulada en estos años como del hecho de que existen nuevas realidades a las que es preciso dar una adecuada respuesta jurídico penal”... “desde la aprobación del C.P. tanto diversas disposiciones de la Unión Europea, proposiciones parlamentarias como la realidad social han provocado que una reforma coherente y sistemática del C.P. tenga que abordar la definición de nuevos tipos legales y la modificación de algunos de los ya existentes, para ser capaces de abordar el problema de la criminalidad en todos sus ámbitos y contribuir también con las reformas a combatir la criminalidad con mayor eficacia e incrementar la seguridad de todos los ciudadanos y el pacífico disfrute de sus bienes y derechos”.

En concreto y referido a delincuencia informática dice que: “Se incorporan las figuras delictivas relacionadas con el acceso a los servicios de radiodifusión sonora o televisiva o servicios interactivos prestados a distancia por vía electrónica. En este caso se hace una minuciosa regulación de las conductas que atentan directa y gravemente contra la prestación de estos servicios, siguiendo también las orientaciones contenidas en las Decisiones de la Unión Europea. Así mismo, se castiga la manipulación de los terminales de equipos de telecomunicación, como en el caso de los teléfonos móviles”.

Las modificaciones del Anteproyecto son las siguientes:

Artículo 186.- De los delitos de exhibicionismo y provocación sexual: se modifica en el sentido de incrementar la pena de multa que pasa de 12 a 24 meses.

Artículo 189.- Dentro de los delitos relativos a la prostitución y la corrupción de menores: se introduce la expresión “cualquiera que sea su soporte”.

Artículo 248.- Dentro de las estafas: se añade un párrafo 3 que dice lo siguiente “3. Los que fabricaren, introdujeran, poseyeran o facilitaren programas de ordenador específicamente destinados a la



comisión de las estafas previstas en este artículo, serán castigados con la pena señalada en cada caso para el supuesto que se trate”.

Artículo 286.- Dentro de los delitos relativos al mercado y a los consumidores, se da una nueva redacción a este artículo que queda como sigue:

“1. Será castigado con las penas de prisión de seis meses a dos años y multa de seis a veinticuatro meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, normalmente contra remuneración, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1º.

2. Con idéntica pena serán castigados quienes, con ánimo de lucro, alteren o dupliquen el número identificativo de equipos de telecomunicación, comercialicen equipos que hayan sufrido alteración fraudulenta y los que con idéntico ánimo, alterar o duplicar cualquier dispositivo lógico o electrónico necesario para el funcionamiento de equipos de telecomunicación en una red determinada sin consentimiento del titular de la red.

3. A quien, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública suministre información a una pluralidad de personas sobre el modo de conseguir el acceso no autorizado a un servicio de los expresados en ese mismo apartado 1, incitando a lograrlo, se le impondrá la pena de multa en él prevista.

4. A quién, utilice los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional se le impondrá la pena prevista en el artículo 255 de este Código con independencia de la cuantía de la defraudación”.

Artículo 287. Relativo a las disposiciones comunes. Se modifica en el sentido que los delitos contra la propiedad intelectual e industrial no exigirán denuncia a instancia de parte, por lo que pasan a ser delitos perseguibles de oficio. Se mantiene únicamente la denuncia de la persona agraviada o de su representantes legales, o del

Ministerio Fiscal cuando se trate de menores de edad, incapaces o persona desvalida, cuando se trate de los delitos relativos al mercado y a los consumidores.

#### 4. Soluciones a nivel internacional y europeo

La cibercriminalidad reúne dos características que hacen que la persecución de un delito sea mas complicado:

- La internacionalización, es decir, frecuentemente la comisión y/o sus efectos se extienden a varios Estados.

- La falta de territorialidad definida. No existen fronteras ni para el origen de la comisión delictiva, ni para la extensión de sus efectos, ni para el recorrido de la transmisión; sobre todo si se tiene en cuenta que cada vez es más habitual que exista un tercer o cuarto Estado donde física y técnicamente se cometen los delitos (son los denominados “paraísos informáticos”, sedes de “hosting” delictivos).

Todo ello unido a que las Jurisdicciones de los distintos Estados pretendan ser competentes para enjuiciar el mismo asunto y que cada uno de ellos definan su jurisdicción con arreglo al clásico principio de territorialidad así como aplicando también principios como el de personalidad activa, protección, personalidad pasiva y el de universalidad (así ocurre en nuestro derecho en virtud del art. 23 de la L.O.P.J.), hace que sea necesario la existencia de normas de Derecho Internacional que resuelvan los conflictos entre las Jurisdicciones Estatales.

### UNIÓN EUROPEA

En el ámbito de la creación de un espacio europeo de justicia, libertad y seguridad (Tercer Pilar), las instituciones de la U.E. están realizando una importante labor en materia de delincuencia informática.

El Consejo Europeo de Tampere (octubre 1999) entendió necesaria una aproximación en materia de cibercriminalidad, con definiciones y sanciones comunes; posteriormente, el Consejo de Feira (2000) estableció el Plan de Acción e-Europe. Es importante el contenido de la Comunicación de la Comisión Europea al Parlamento y al Consejo sobre seguridad de los sistemas de redes y de lucha contra la delincuencia informática (Comunicación “Seguridad de las redes y de la información –Propuesta para un enfoque político europeo” de 6 de junio de 2001), que se refiere tanto a la seguridad en Internet, necesaria para el desarrollo del comercio electrónico, como a la lucha contra la criminalidad en este ámbito.

Entre las iniciativas llevadas a cabo por la Comisión Europea destaca la siguiente:

Propuesta de Decisión-Marco relativa a los ataques de los que son objeto los sistemas de información, de 19 de abril de 2002, que de una



parte, incorpora penas privativas de libertad de entre uno y cuatro años para las conductas relativas a ataques a sistemas informáticos, en los que se incluyen los accesos inconsentidos cometidos contra una parte de un sistema de información que es objeto de medidas de protección especiales y que de otra, prevé, como circunstancias agravantes, que el delito se cometa por una organización criminal o que se causen daños físicos a personas o daños sustanciales a infraestructuras sensibles o vitales de un país.

En julio de 2002 se remitió al Parlamento Europeo para el correspondiente dictamen. En Agosto de 2002, se han presentado dos proyectos, uno de informe (29 de agosto) y otro de opinión (2 de agosto).

Por otro lado, también es importante mencionar la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que autoriza a los Estados miembro a que regulen por ley la obligación a cargo de los prestadores de servicios de conservar los datos electrónicos de tráfico de sus clientes, por razones de seguridad nacional, defensa, seguridad pública y de lucha contra la criminalidad, durante un tiempo limitado, que cada gobierno puede establecer a su arbitrio.

### **Ámbito Internacional**

46

En el seno del Consejo de Europa se ha elaborado como iniciativa el Convenio sobre la Ciberdelincuencia o Convenio sobre el Cibercrimen, fue abierto a la firma en Budapest en noviembre de 2001. Lo han firmado un total de 34 países, entre ellos España, y está pendiente de ratificación por cinco Estados, 3 de ellos al menos, miembros del Consejo de Europa, para que entre en vigor.

Dicho Convenio consta de un Preámbulo y cuatro capítulos, divididos éstos a su vez en secciones y subdividido en títulos.

El capítulo I, establece las definiciones que han de entenderse por “sistema informático” y por “datos informáticos”.

El capítulo II, establece las medidas legislativas que han de adoptar los Estados parte, referidas tanto en el ámbito del derecho penal sustantivo (Sección 1) como en el ámbito procesal (Sección 2).

Los objetivos principales de este convenio son dos:

1º) Instar a los Estados parte a tipificar como delito una serie de conductas relacionadas con la informática y las redes de comunicación, como el acceso no autorizado a un ordenador, la difusión por vía electrónica de pornografía infantil o las violaciones de los derechos de propiedad intelectual que se comentan en dichas redes.

2º) Establecimiento de medidas procesales o cautelares adaptadas al medio digital, que faciliten la detección, la investigación y la obtención de pruebas de infracciones contra o mediante un sistema informático o cuyas fuentes de pruebas se hallen en soporte electrónico. Estas medidas se concretan en las siguientes: la conservación inmediata de datos almacenados, el mandato de comunicación, el registro y decomiso de datos informáticos almacenados y la recogida en tiempo real de datos informáticos.

## SOLUCIONES A NIVEL NACIONAL

a) Real Decreto Legislativo 1/1996, por el que se aprueba el texto refundido sobre propiedad intelectual.

Este texto, desarrolla una serie de medidas para combatir la piratería informática, como la posibilidad de que los fabricantes de programas de ordenador soliciten a la justicia española la realización de un registro sorpresa en empresas en las que existan sospechas fundadas o evidencias de un delito. España es uno de los países en los que se puede acudir a esta medida cautelar. De esta manera se erradica la posibilidad de que los presuntos infractores puedan destruir las pruebas existentes, lo cual, indudablemente ocurriría si se les notifica por adelantado la realización de un registro.

b) Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE).

47

La LSSICE incorpora algunos de los instrumentos de persecución de delitos que se recogen en el Convenio sobre la Ciberdelincuencia, así como también algunos aspectos regulados en la Directiva 2002/58/CE, de 12 de Julio, sobre privacidad y las comunicaciones electrónicas.

Por un lado impone a los prestadores de servicios un deber de colaboración con las autoridades públicas (tanto administrativas como judiciales). En virtud de este deber se podrá ordenar, por órgano competente, a dichos prestadores que suspendan la transmisión, el alojamiento de datos, el acceso a las redes de telecomunicaciones o la prestación de cualquier otro servicio equivalente de intermediación que realicen.

Además se establece un apoderamiento a las autoridades públicas para exigir a los prestadores de servicios de intermediación que cooperen en la ejecución de resoluciones judiciales o administrativas. La atribución de esta facultad se justifica por la dificultad, en muchos casos, de identificar a los prestadores finales de servicios y la posición más ventajosa de los prestadores de intermediación, al actuar como puerta de acceso a los contenidos, para localizar el origen de las comunicaciones e interrumpir su continuación, si así se ordenara. Todo ello sin olvidar que cuando se trate de medidas que incidan y restrinjan derechos fundamentales, deben éstas ajustarse en su adopción y cumplimiento a las garantías, normas y procedimientos previstos por el ordenamiento jurídico (art.11.2 primer y segundo párrafo).



De otro, la LSSICE regula un deber de retención de datos de tráfico, para asegurar que, cuando los órganos judiciales o la Fuerzas y Cuerpos de Seguridad del Estado van a iniciar una investigación penal, puedan averiguar el origen de una comunicación presuntamente delictiva. La conservación de dichos datos es necesaria, ya que normalmente la investigación criminal no se desarrolla de forma simultánea a la comisión del delito, sino con posterioridad.

Se distinguen dos supuestos según la actividad desempeñada por el prestador:

Artículo 12.2 primer y segundo párrafo:

1º) Operadores de redes y servicios de comunicaciones electrónicas y los proveedores de acceso a redes de telecomunicaciones: estos deberán conservar los datos necesarios para facilitar la localización del equipo terminal (IP del ordenador).

2º) Prestadores de servicios de alojamiento de datos, retendrán aquellos imprescindibles para identificar el origen de los datos alojados y el momento en que se inició la prestación del servicio.

48

El objetivo primordial del deber de retención reside, sin duda, en facilitar la represión —y por tanto, la previa detección, investigación y prueba— de los ilícitos perpetrados en la red. Según dice el legislador en el art.12.3 la finalidad de la retención de datos es la posibilidad de utilizar los mismos en el marco de una investigación criminal.

En ningún caso el deber de retención afectará al secreto de las comunicaciones, no recaerá sobre datos de contenido ni sobre datos de navegación y el plazo máximo de conservación de datos será de doce meses.

La LSSICE garantiza además, que la custodia de esos datos se efectúe con arreglo a lo dispuesto en la normativa sobre protección datos personales y que el acceso a los mismos se haga siempre bajo control judicial o del Ministerio Fiscal.

Por último, esta ley, regula también un régimen especial de responsabilidad de los prestadores de servicios de intermediación. Dicho régimen no es excluyente de las demás responsabilidades civiles, penales y administrativas en que pudieran incurrir en virtud de otras normas, como dice el artículo 13.

## MEDIDAS PROCESALES

El Derecho Procesal Penal no contiene disposiciones especiales en materia de investigación y enjuiciamiento de delitos informáticos, por lo que las especiales dificultades para la obtención de la prueba generadas por este tipo de delitos deben ser abordadas mediante la aplicación de los medios procedimentales ordinarios. En este ámbito, los principales problemas se refieren a dos cuestiones: la propia obtención de la prueba; y el mantenimiento de la cadena de custodia.

### La obtención de la prueba

En relación con esta cuestión, es importante la intervención de las comunicaciones (especialmente de los correos electrónicos). El ordenamiento jurídico permite esta posibilidad por la aplicación de las normas de las intervenciones telefónicas (arts.579 y concordantes de la LECRIM): autorización previa y control posterior por parte del juez de Instrucción, motivación de la resolución autorización, y principio de proporcionalidad.

Sin embargo, la internacionalización y falta de territorialidad que caracteriza a este tipo de delitos determinan la necesidad de realizar una intervención de las comunicaciones que afecten a varios Estados.

La vía clásica de la comisión rogatoria resulta actualmente claramente insuficiente e ineficaz.

49

En el ámbito de la Unión Europea debe destacarse la regulación de la intervención de las telecomunicaciones contenida en el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembro de la Unión Europea, aprobado por Acto del Consejo de 29 de Mayo de 2000.

Dicho convenio regula la intervención de las “telecomunicaciones”, debiendo interpretarse tanto las telefónicas como cualquier otro tipo de comunicación que permitan las tecnologías actuales y futuras.

Respecto de este convenio, recientemente, el Pleno del Senado, en sesión de 10 de Junio de 2003, ha aprobado a efectos de lo dispuesto en el artículo 94.1 de la C.E., la Declaración de Aplicación Provisional del Convenio de asistencia judicial en materia penal entre los Estados miembro de la Unión Europea, hecho en Bruselas el 29 de mayo de 2002, sin introducir variaciones en el texto remitido por el Congreso.

Asimismo, esta misma Declaración de Aplicación Provisional la han aprobado dos países más: Portugal y Dinamarca.

### Mantenimiento de la cadena de custodia

La investigación de los delitos a través de Internet debe reproducir la ruta electrónica seguida por el autor para la comisión del delito. De esta manera, será necesario recoger los datos (objeto o producto del delito)



salvaguardar los correspondientes en los servidores e ISPs (proveedores de acceso y servicios de Internet), recorrer en sentido contrario el camino del delincuente y, por último, relaciones del equipo informático utilizado con la persona física autora. Solamente de esta manera podrá conocerse quién ha realizado una operación económica fraudulenta a través de Internet, o quién ha colgado un vídeo pornográfico infantil en la Red. Por todo ello, resulta muy importante adoptar garantías para asegurar la cadena de custodia de los datos anteriormente citados.

No obstante, resultará dificultoso el establecimiento de la relación final entre el equipo informático desde el cual se cometió el delito y la persona física que lo utilizó; a estos efectos deberán utilizarse las técnicas clásicas de investigación policial del delito, siendo muy importante la colaboración ciudadana y de las empresas del sector.

### NECESIDAD DE CONOCIMIENTOS ESPECIALIZADOS

En esta materia resulta estrictamente necesario que las autoridades y agentes encargados de la persecución del delito cuenten tanto con conocimientos especializados, como con el debido asesoramiento de expertos o peritos. Y ello por las siguientes razones.

50

El desconocimiento general de los medios utilizados, e incluso de sus implicaciones en la vida cotidiana.

La constante evolución de las tecnologías en los servicios: telefonía móvil, acceso a internet, e-mail, chats, accesos por satélite, reconocimiento de voz, etc..

La propia evolución de las tecnologías de ataque y vulneración: ocultación de identidad, desvíos de llamadas fraudulentas, programas de averiguación de palabras clave, escaneo, virus, gusanos, bombas lógicas, envíos y recepciones no deseados de ficheros con pornografía infantil, etc..

Por otro lado, así como en la fase de investigación se cuenta con unidades policiales especializadas en esta materia, no existe ninguna especialización de Jueces ni del Ministerio Fiscal (hubo una propuesta por el Senado de configurar fiscalías especializadas en esta materia).

En la fase de enjuiciamiento, resulta relevante la existencia de adecuados peritajes o dictámenes técnicos.

(\*)En marzo de 2000 se creó la Unidad de Investigación de la Delincuencia en Tecnologías de la Información, que funcionalmente cuenta con cuatro grupos operativos para la persecución de los fraudes contra las comunicaciones; fraudes en Internet; pornografía infantil e infracciones contra el honor y contra los derechos de autor y seguridad informática.

Existen alrededor de 35-40 funcionarios en el Cuerpo Nacional de Policía dedicados a las tareas de investigación de los ilícitos cometidos en la Red.

Respecto a la evolución de estos medios personales así como de medios materiales se han quintuplicado desde 1996 hasta el año 2002.

En la Dirección General de la Guardia Civil también se ha creado un Grupo dedicado a la Investigación de Delitos de Alta Tecnología, entre cuyos cometidos se encuentra la lucha contra la delincuencia que utiliza la red para la realización de sus actividades ilícitas. Se está contemplando la reordenación de determinadas Unidades de Policía Judicial de Zonas, de forma que se recupere personal para reforzar aquellos órganos considerados de más necesaria potenciación, como es el caso del referido Grupo de Alta Tecnología (los componentes de estos grupos participan en reuniones internacionales de Interpol y Europol para establecer planes de colaboración en el campo de la delincuencia informática).

En la lucha contra el ciberdelito se están realizando importantes esfuerzos como los realizados en el año 2002 de establecer conexiones de varias Comandancias y Puestos a la Red, Unidades a las que se ha dotado de nuevo material informático y de nuevas conexiones informáticas.

También se ha formado un Departamento de Electrónica e Informática (dentro del Centro de Investigación y Criminalística del Servicio de Policía Judicial) para la peritación de material incautado en relación con los delitos informáticos, así como el desarrollo de investigaciones criminalísticas en este ámbito forense.

La inversión realizada en el año 2002 fue de 38.000 euros para su dotación.

El gobierno ha emprendido actuaciones para implantar un Plan de Seguridad en la Red, a través del Ministerio de Ciencia y Tecnología en coordinación con otros Ministerios. Destacamos las siguientes:

Campañas de prevención y difusión de información sobre protección frente a virus informáticos y, en general, sobre seguridad en Internet.

Iniciativas normativas:

Ley 34/2002, de Servicios de la Sociedad de la Información y de Comercio Electrónico

Ley de Firma Electrónica

Actualmente está en elaboración un proyecto de Real Decreto sobre interceptación legal de las comunicaciones electrónicas, regulándose las actuaciones de las Fuerzas y Cuerpos de Seguridad del Estado en la per-



secución de delitos que utilizan medios electrónicos de comunicación, como por ejemplo la Red Internet

(\*) Extraído de la contestación de una pregunta parlamentaria a la Presidencia del Senado.

## PROYECTOS FUTUROS

Por las características que rodean a este tipo de delincuencia informática, su internacionalización y falta de territorialidad, así como el riesgo de desaparición tanto de las pruebas como de los productos del delito (por la gran facilidad de las comunicaciones debido a la creciente potencia de los medios informáticos), es necesario el acercamiento o aproximación de los distintos ordenamientos nacionales, adoptando definiciones y medidas comunes.

En este sentido aparte del mencionado Convenio sobre la ciberdelincuencia, se pueden mencionar los siguientes proyectos:

La Comisión Europea ha creado un borrador de ley para armonizar en la UE la legislación sobre el cibercrimen.

Propuesta de Decisión-Marco para unificar tipos de delitos y penas de piratería informática (previsión de que entre en vigor antes de 2004).

## BIBLIOGRAFÍA CONSULTADA

ÁLVAREZVIZCAYA,MAITE. "Consideraciones político criminales sobre la delincuencia informática: El papel del derecho penal en la red". Cuadernos y Estudios de Derecho Judicial. C.G.PJ Año 2002.

ÁLVARO A, SÁNCHEZ BRAVO. "Espionaje en el Ciberespacio".

DAVARA RODRIGUEZ, MIGUEL ÁNGEL. "Informática y Derecho". Tomos I y II (1987 a 2002).

GARCÍA RUÍZ, JOSÉ MARIANO. "Correo electrónico y proceso penal". Diario La Ley nº 5805 de 18-06-03.

HERNÁNDEZ GUERRERO, FJ y ÁLVAREZ DE LOS RIOS, JOSÉ LUIS. "Medios informáticos y proceso penal". Página web de Fiscalía.

LAGARES GARCIA, DIEGO. "Internet y el Derecho". Ediciones Carena 2000.

LEZERTÚA RODRÍGUEZ, MANUEL. "El proyecto de Convenio sobre el Cybercrimen del Consejo de Europa". Cuadernos y Estudios de Derecho Judicial. C.G.PJ Año 2002.

MARCHENA GÓMEZ, MANUEL. "Algunos Aspectos Procesales de Internet". Página WEB de Fiscalía.

MORÓN LERMA,ESTHER. "Internet y Derecho Penal: Hacking y otras conductas en la Red". Ed.Aranzadi. 2002

REYNA ALFARO, LUIS MIGUEL. "La criminalidad informática: cuestiones para una reflexión inicial". Revista de Actualidad Penal. Nº 21. Semana del 20 al 26 de mayo de 2002.

ROVIRA del CANTO, ENRIQUE. "Delincuencia informática y fraudes informáticos". Estudios de Derecho Penal dirigidos por Carlos María Romeo Casabona. Editorial Comares. 2002.



## **INICIATIVAS POLÍTICAS EUROPEAS PARA MEJORAR LA SEGURIDAD DE LA SOCIEDAD DE LA INFORMACIÓN**

**Danny de Temmerman**  
**Administrador. Dirección General de**  
**la Sociedad de la Información.**  
**Unión Europea**

Permítanme decirles que me siento enormemente honrado por encontrarme aquí con ustedes hoy, el último día del Seminario sobre el presente y el futuro de la seguridad de la Sociedad de la Información. Me gustaría dar las gracias a los organizadores por ofrecerme la oportunidad de hablar acerca de los esfuerzos que la Comisión Europea está llevando a cabo para ayudar a crear una Sociedad de la Información más segura, mejorando la seguridad de las redes y las infraestructuras de información y combatiendo los delitos informáticos.

55

La seguridad de las redes y las comunicaciones es un área de interés muy importante para el desarrollo de la Sociedad de la Información y para la creación de un área de seguridad dentro de la Unión Europea. Los sistemas y redes de información en este momento están dando apoyo a servicios y están transportando datos de gran valor que pueden ser vitales para otras infraestructuras de importancia fundamental. Por tanto, las redes y los sistemas de información necesitan una protección cada vez mayor contra los ataques a su disponibilidad, autenticidad, integridad y confidencialidad. El mal funcionamiento de las redes y sistemas de información afecta a todos: ciudadanos, empresas y administraciones públicas.

Como consecuencia de la posibilidad de conexión ofrecida por las infraestructuras de comunicaciones electrónicas, las infraestructuras convencionales como transporte, energía, sanidad, servicios financieros y comercio están siendo cada vez más interdependientes. El uso cada vez más frecuente de las infraestructuras de comunicación "abiertas", como Internet, y el empleo generalizado de aplicaciones de programas concretos también tienen un impacto en cuanto a la veracidad. Estas evoluciones

permiten la introducción de nuevas vulnerabilidades y amenazas, tanto accidentales como deliberadas.

La evolución de la política en relación con la protección de infraestructuras críticas de información hoy, es una actividad importante desarrollada por los Estados miembro. La Comisión Europea interviene cuando se pueden obtener ventajas del incremento de la coordinación y de la armonización de las políticas de los Estados miembro para garantizar el correcto funcionamiento del mercado interno.

La protección de la infraestructura crítica de la información es una responsabilidad de muchas facetas que tiene que ser desempeñada de forma conjunta por el gobierno y el sector privado. La industria, por supuesto, tiene un papel clave que desempeñar en este campo, especialmente cuando la mayoría de las redes son de titularidad y gestión privada.

Teniendo en cuenta también la experiencia obtenida en el periodo subsiguiente a los acontecimientos del 11 de septiembre, el Plan de Acción e-Europe 2005, acordado en Sevilla el año pasado, promovía el incremento de la acción en el área de la seguridad de la información y de las redes. Se consideró importante la necesidad de establecer una estructura a nivel de la UE para ayudar a los Estados miembro y a las instituciones europeas en sus esfuerzos para mejorar la seguridad de las redes y los sistemas de información.

56

Estas necesidades sin precedentes de una mejor seguridad informática deben compaginarse asimismo con la confianza y responsabilidad pública, fundamental en cualquier sociedad abierta. Esto será necesario para proteger la privacidad, compartiendo recursos informáticos a la vez que asegurando la veracidad de los productos y servicios.

### **ACTIVIDADES ACTUALES DE LA COMISIÓN EN EL CAMPO DE LA SEGURIDAD INFORMÁTICA**

Las actividades actuales de la Comisión en el campo de la seguridad Informática en el panorama general de la "seguridad informática", se pueden clasificar en tres amplias categorías:

- En primer lugar tenemos establecido el marco legislativo sobre telecomunicaciones y protección de datos.
- En segundo lugar, estamos garantizando un seguimiento legislativo específico de la estrategia contra los delitos informáticos lanzada en 2001.
- En tercer lugar, las actividades sobre seguridad de redes e información completan el panorama.



## El nuevo marco electrónico de comunicaciones

Se aproximan algunas fechas importantes para el nuevo marco de comunicaciones electrónicas, que entrará en vigor este mes. Este marco legislativo contiene disposiciones y obligaciones de los Estados miembro y operadores que garanticen la disponibilidad, integridad y confidencialidad de las comunicaciones electrónicas. Los Estados miembro implementarán la nueva directiva de protección de datos el próximo mes de octubre. Ya no hay distinción entre datos que viajan a través de redes tradicionales y los que llegan a su destino utilizando Internet.

En el área de las comunicaciones no solicitadas, la Directiva hace que la tecnología de las disposiciones relevante sea neutral y armoniza los diferentes regímenes nacionales para el tratamiento del spam(1). Creo que tendremos interesantes debates sobre el problema del spam en los próximos meses, ya que es uno de esos asuntos que requiere soluciones globales.

## Iniciativas contra los delitos informáticos

La delincuencia informática está creciendo rápidamente. Un informe reciente publicado por Symantec descubrió que la compañía experimentó una media de 30 ataques informáticos a la semana durante los últimos seis meses de 2002. Con el comercio de Internet en la UE se espera que aumente de los 271,5 billones de Euros en 2002, a 828,9 billones de Euros en 2004, incluso los ataques menores o insignificantes pueden tener un efecto devastador. Por dar un ejemplo: el virus Código Rojo ha tenido un impacto económico global negativo de 2,5 billones, mientras que el Love Bug ha ocasionado más de 8 billones de euros en pérdidas financieras.

También existe una creciente preocupación acerca de los criminales organizados que lanzan ataques contra los sistemas de información para su propio beneficio. Los grupos piratas organizados, especializados en la piratería y la desconfiguración de sitios web se encuentran cada vez más activos a nivel mundial, por ejemplo intentando extorsionar a sus víctimas ofreciéndoles asistencia especializada después de introducirse ilegalmente en sus sistemas de información. De hecho, un estudio reciente concluyó que el crimen organizado constituye el 13 por ciento de los ataques de delitos informáticos contra la industria(2).

El terrorismo informático es otra amenaza y debe ser tenido mucho más en cuenta después de los trágicos acontecimientos del 11 de septiembre. Ha habido numerosas ocasiones en las que las relaciones internacionales han llevado a ataques masivos contra los sistemas de información, a menudo incluyendo ataques contra web-sites. Los ataques más importantes y mejor organizados no sólo podrían llevar a importantes perjuicios financieros, sino en algunos casos, podrían llevar incluso a la pérdida de vidas, por ejemplo un ataque contra las redes utilizadas por un hospital o un sistema de control de tráfico aéreo. Se pueden imaginar los daños.

1.- N. de la t.- Publicidad no deseada en Internet

2.- Encuesta de Delitos informáticos 2001. Confederación de la Industria Británica (ver <http://www.cbi.org.uk>)



Por tanto, existe una razón importante para adoptar medidas preventivas para evitar y reaccionar a estos ataques.

La seguridad global de la redes también puede mejorarse garantizando que los Estados miembro dispongan de los medios legislativos apropiados para prevenir y combatir cualquier forma de actividad criminal contra las redes.

En 2001, la Comisión publicó una Comunicación sobre el tema “Crear una sociedad de la Información más segura mejorando las infraestructuras de seguridad de la información y combatiendo los delitos relacionados con la informática”. Esta comunicación fue patrocinada conjuntamente por los Comisarios Antonio Vitorino, responsable de Justicia y Asuntos de Interior y Erkki Liikanen, responsable de la Sociedad de la Información. Fue el primer documento de política europea en materia de delitos informáticos y sirvió como base para discusiones posteriores. Contenía un número importante de iniciativas.

Una de las iniciativas anunciada en esta Comunicación fue una Decisión Marco sobre ataques contra sistemas de información. La Comisión Europea la propuso hace un año. El 28 de febrero de 2003, el Consejo de la Unión Europea alcanzó un acuerdo político sobre el texto. Confío en que la propuesta será adoptada en breve plazo, ya que todos los Estados miembro excepto uno (Suecia), dejaron a un lado sus reservas parlamentarias.

La Decisión Marco garantizará un nivel mínimo común de aproximación al derecho penal para las formas más importantes de actividad criminal contra los sistemas de información, tales como acceso ilegal, sistema ilegal e interferencia de datos. Esto incluye la llamada “piratería informática” y “ataques de denegación de servicio”, así como la difusión de códigos y virus perjudiciales.

Esta aproximación es conveniente con el fin de evitar cualquier vacío en los sistemas jurídicos de los Estados miembro, que podría obstaculizar la respuesta de las autoridades policiales y judiciales, a nivel nacional, a estas amenazas crecientes.

Por otra parte, la naturaleza transnacional de la piratería informática, los virus y los ataques de denegación de servicio, significa que en este área es absolutamente fundamental la cooperación efectiva policial y judicial entre los Estados miembro de la Unión Europea, así como con los países no pertenecientes a la Unión Europea.

Además, la cooperación internacional mejorará garantizando que los Estados miembro cuenten con disposiciones de derecho penal que les permita responder a las peticiones de cooperación procedentes de otros países. La Decisión Marco también garantizará que los Estados miembro cuenten con las facultades jurisdiccionales apropiadas para emprender acciones, y contiene disposiciones sobre la responsabilidad de las personas jurídicas.

Este estudio es complementario a la propuesta de la Agencia para Seguridad de las Redes e Información, que trata de medidas de seguridad preventivas; la Decisión Marco trata de investigaciones criminales posteriores.

Considero que éste es un paso importante para conseguir evitar la existencia de los llamados “refugios del crimen” en Europa.

### **OBJETIVOS DE LA AGENCIA PARA LA SEGURIDAD DE LAS REDES E INFORMACIÓN (NISA)**

Quisiera ahora compartir con ustedes algunas impresiones acerca de la propuesta de la Comisión estableciendo una Agencia Europea para la Seguridad de las Redes e Información (NISA), que es uno de mis proyectos trabajando para la “Dirección General de la Sociedad de la Información”.

Ya he manifestado antes cómo la seguridad de las redes e información se ha convertido en una preocupación importante, especialmente en el periodo subsiguiente a los acontecimientos del 11 de septiembre. Sin embargo, los Estados miembro se encuentran en diferentes fases de su trabajo encaminado a la mejora de la seguridad de las infraestructuras de información y los enfoques varían. Hoy en día no existe cooperación transfronteriza sistemática en materia de seguridad de las redes e información entre los Estados miembro, aunque la seguridad no puede ser un asunto aislado únicamente para un país.

El Parlamento Europeo, el Consejo y la Comisión recomiendan una coordinación europea más estrecha en materia de seguridad de la información. La Unión Europea se beneficiará de la creciente coordinación entre los Estados miembro para conseguir un nivel suficientemente alto de seguridad en todos ellos, contribuyendo al mismo al funcionamiento del mercado interno.

Por tanto, la Comisión ha propuesto la creación de una Agencia para la Seguridad de las Redes e Información para unir los esfuerzos para mejorar la seguridad de las redes e información y para incrementar la capacidad de los Estados miembro y las instituciones de la UE para prevenir y responder a los problemas importantes de seguridad de las redes e información.

En última instancia, la Agencia servirá como centro de conocimientos donde los Estados miembro y las instituciones de la UE puedan buscar asesoramiento sobre materias relacionadas con la seguridad. Estos conocimientos proporcionados por la Agencia, junto con el objetivo de instalar una cultura de seguridad en Europa, desempeñarán un papel clave para la seguridad de la economía digital de Europa, y el desarrollo de la sociedad de la información en general.



## Cometidos de la Agencia

Los cometidos propuestos de la Agencia consisten en funciones de asesoramiento y coordinación. Actualmente, tanto las organizaciones públicas como privadas recogen datos sobre incidentes de tecnología de la información y otros datos relevantes para la seguridad de la información con diferentes objetivos. Sin embargo, no existe una entidad central a nivel europeo que analice estos datos para apoyar la obra de la política de la UE en ese área, y al mismo tiempo proporcione un valor añadido a las iniciativas nacionales.

El aumento de la sensibilización y la cooperación es clave en este área. La Agencia debe estar capacitada para lanzar iniciativas de cooperación entre los diferentes actores en el campo de la seguridad de la información, por ejemplo, apoyar el desarrollo del comercio electrónico seguro. Por consiguiente, es necesaria la participación y la implicación de todos los actores de la asociación pública /privada. Por supuesto que la industria tiene un papel clave que desempeñar en este campo, especialmente teniendo en cuenta que la mayoría de las redes son de propiedad privada y gestionadas por entidades privadas.

La iniciación de un estudio europeo coordinado y la promoción de métodos de valoración y gestión de riesgos mejorará nuestra capacidad para hacer frente a las crecientes amenazas para la seguridad de la información.

60

No únicamente los requisitos legales pueden afectar a la seguridad de productos y servicios, sino también, en gran medida, las necesidades técnicas, la Agencia realizará esfuerzos de estandarización. Esto se efectuará en estrecha colaboración con la industria y basándose en su experiencia.

## Asociación Unión Europea - Estados Unidos

Sabemos que los temas de seguridad de las redes y de la información son mundiales, ya que los canales de comunicación electrónicos no se detienen en las fronteras nacionales ni europeas. Es necesario incrementar la cooperación internacional en este campo. La Agencia facilitará apoyo para los contactos europeos con las partes pertinentes de terceros países.

Quisiera aquí hacer referencia a los esfuerzos realizados por nuestros colegas estadounidenses. En febrero de este año han publicado una Estrategia Nacional para proteger el ciberespacio, ésta se basa en una asociación extremadamente elaborada entre el sector público /privado.

Para poner en marcha la Estrategia Nacional, el Secretario Ridge ha anunciado hace dos semanas la creación de la "División de Seguridad Informática Nacional" (NCSD) encuadrada dentro del Departamento de Estados Unidos de Seguridad de la Patria. La División identificará, analizará y reducirá las amenazas informáticas y vulnerabilidades, diseminará información de aviso de amenaza, coordinará la respuesta de incidentes y facilitará asistencia técnica en el avance de operaciones y programación de la



recuperación. Trabajaré en estrecha asociación con la industria y otras asociaciones en este área crítica.

Estamos seguros que, una vez que se haya implementado NISA, representará junto con los departamentos asociados de la Comisión el socio natural de esta nueva División. La cooperación transatlántica resultará considerablemente beneficiada en el área de la Seguridad de las Redes y de la Información.

## CONCLUSIÓN

El Consejo Europeo de Primavera pidió la adopción de la Decisión Marco en materia de ataques contra los sistemas de información como muy tarde en Junio de 2003 y la creación de una Agencia Europea para la Seguridad de las Redes e Información a finales del 2003. Para cumplir con estas fechas fijadas, los Consejos del JAI y Telecom ya han adoptado una propuesta general sobre ambas iniciativas.

La Comisión ve esto como una señal importante para continuar trabajando de forma constructiva junto con el Parlamento Europeo y el Consejo para tener un acuerdo formal a tiempo para respetar las fechas límites impuestas por el Consejo Europeo.

La seguridad de las redes y de la información es un elemento esencial de nuestras vidas diariamente. La sociedad, de forma global, al igual que los individuos tiene que aprender cómo gestionar los riesgos que conllevan las redes y los sistemas de información.

Confío que las dos iniciativas de la Comisión contribuirán a ese proceso que redunde en el beneficio de los ciudadanos y la industria europea.

También quisiera dar las gracias a los funcionarios del gobierno español y representantes del sector privado que han contribuido positivamente en los debates políticos sobre estos importantes temas de seguridad.

# **SOCIEDAD DE LA INFORMACIÓN Y SEGURIDAD**

**Manuel Aguilar Seco**  
**Inspector del Cuerpo Nacional de Policía**

El desarrollo imparable de las telecomunicaciones, de la informática e Internet, está configurando una nueva sociedad, la de la información. Su carácter incipiente y evolución vertiginosa, la rapidez con la que se incorporan al mercado los nuevos avances tecnológicos, la ausencia de fronteras y de límites a un espacio virtual que rompe los esquemas tradicionales de espacio/tiempo, unido a su ámbito global, conforman una sociedad llena de vulnerabilidades y de oportunidades para la delincuencia.

63

La concurrencia de estos factores, la creciente dependencia tecnológica de todos los sectores sociales y productivos, el reconocimiento de que la tecnología de la información y la comunicación constituye un factor decisivo para crear una economía mundial basada en el conocimiento y la competitividad de las empresas y para alcanzar el desarrollo y la integración de todos los países; obliga a la eliminación de los déficits de seguridad que pueden dificultar o, en su caso, impedir esos objetivos.

La seguridad constituye, por tanto, un factor prioritario clave, para generar confianza. La delincuencia cibernética no puede ser el obstáculo que impida el progreso y el bienestar del ciudadano. Se hace preciso y necesario un esfuerzo por parte de todos para poder identificar esos déficits, evaluar riesgos y oportunidades y analizar y configurar las respuestas más eficaces y adecuadas.

Esa necesidad de seguridad se evidencia en el crecimiento que en los últimos años han tenido y tendrán los productos para asegurarla. Según algunos estudios, el mercado mundial de programas informáticos de seguridad para Internet se estimó en 1999 en 4,4 millardos de dólares y para el



2004 se prevé que esa cifra llegue a los 8,3. En Europa, se considera que el mercado de la seguridad de las comunicaciones electrónicas pasará de 465 millones de dólares en 2000 a 5,3 millardos de dólares en 2006.

## **SOCIEDAD DE LA INFORMACIÓN. DEFINICIÓN. CARACTERÍSTICAS. TECNOLOGÍA Y USO**

Esta Sociedad se configura en el espacio electrónico y se define como "aquella que utiliza de forma intensiva y extensiva las tecnologías de la información y la comunicación". Se caracteriza por:

- El papel fundamental que adquiere la información. La información se erige como la materia prima por excelencia y la tecnología se desarrolla para su gestión. En este tipo de sociedad la posición e influencia, tanto del individuo como de las organizaciones, se mide por la cantidad de información y conocimientos que posean. Información y conocimientos son la base para producir riqueza y servicios y mejorar de forma sustancial los que ya se prestan.

- La globalidad y descentralización. La idea del espacio/tiempo que venimos manejando hasta ahora se diluye. El espacio no tiene fronteras y el tiempo se reduce espectacularmente. Para comprobarlo contemos los segundos que tardamos en localizar y visitar alguna página web de Australia, por ejemplo, o en mandar un correo electrónico o en llamar por teléfono.

- Interconexión. Todo el sistema está interconectado, integrado, armonizado. Entrelazado con el desarrollo de la Sociedad de la Información va el proceso de globalización, basado en la conectividad. La conectividad permite y genera velocidad. Cuanto más conectados estamos más rápidas pueden realizarse las tareas. Así, por ejemplo, en el Cuerpo Nacional de Policía no hay un puesto policial sin Intranet, lo que permite una actualización y coordinación constante, el intercambio de información y el fácil acceso a las bases de datos.

- Dinamismo y flexibilidad. Los cambios son continuos, lo que obliga a una reconfiguración permanente de los sistemas y a una gran flexibilidad organizativa. Como consecuencia de ello la organización en red se presenta como la más eficaz en la Sociedad de la Información. La estructura en red, reticular, genera o permite flujos rápidos de información y la creación de equipos de trabajo pluridisciplinares e interorganizacionales, entre otras ventajas. Hoy día cualquier organización que quiera obtener resultados eficaces necesita de una visión reticular de los problemas. Pero esta nueva

organización en red, también es empleada por los grupos criminales que estructurados de esta manera son más operativos y eficaces, a la vez que les permite actuar simultánea e impunemente, dificultando su localización.

La definición que anteriormente se daba de Sociedad de la Información no reflejaba, no transmitía su verdadera dimensión. Su significado, importancia y dimensión real aparece cuando analizamos e identificamos más detenidamente los "aparatos" que la configuran o componen. De esta manera podemos percibir mejor lo integrados que estamos en ella y la dependencia que tenemos de los mismos: la televisión en sus distintas modalidades -analógica, digital, cable...-, el vídeo, el DVD, el fax, los "buscas", la radio, la cámara fotográfica, la videoconsola, el teléfono fijo y móvil, la informática -ordenadores, periféricos...-, las agendas electrónicas... forman parte ya de nuestra vida.

La importancia e implantación en España de estas tecnologías se constata en una serie de datos extraídos de la "Encuesta a hogares españoles sobre tecnologías de la información y la comunicación. Informe definitivo (mayo de 2003)" de la Comisión del Mercado de las Telecomunicaciones. Así, conocemos que existen 12.368.460 hogares con teléfono fijo, lo que significa que el 90,20% del total de hogares disponen de él. Respecto al móvil la cifra absoluta de hogares que lo tienen se sitúa en 8.917.669, lo que representa que lo hay en 7 de cada 10. En cuanto a su uso, lo utiliza más de la mitad de la población española (18.825.000) mayor de 16 años. En relación con los equipamientos de audiovisuales el 99,55% de los hogares tienen televisión, por ejemplo.

Pero si todos estos datos reflejan la alta penetración de la tecnología en nuestras casas, el futuro que se avecina, si consideramos los distintos proyectos y programas que las diversas administraciones europeas y españolas tienen previsto desarrollar, será aún más tecnológico. Así, para el año 2005 la Unión Europea deberá contar con: unos servicios públicos en línea; una administración electrónica; unos servicios electrónicos de aprendizaje y de salud y un entorno dinámico de negocios electrónicos para crear una economía del conocimiento y una Europa más competitiva. Para ello se pretende duplicar la penetración de Internet en los hogares, renovar el marco de las telecomunicaciones, disminuir el precio del acceso a Internet y facilitar la conexión de casi todas las empresas y centros escolares. También se busca que Europa cuente con la red de investigación más rápida del mundo. Se creará el marco jurídico del comercio electrónico, se aumentarán los servicios de la administración en línea, se acelerará la aparición de una infraestructura de tarjeta inteligente y, para conseguirlo, se establecerá un acceso de banda ancha ampliamente disponible a precios competitivos.



Pero la consecución plena de todos esos objetivos no se alcanzará si no se genera una infraestructura segura. Por ello la Unión ha puesto en marcha una estrategia global basada en la seguridad de las redes, la lucha contra la ciberdelincuencia y la protección de datos electrónicos. En este campo, entre las iniciativas más destacadas se encuentran: el establecimiento de un grupo operativo sobre ciberseguridad; las campañas de sensibilización; la promoción de las buenas prácticas y la mejora de los mecanismos de intercambio de información.

## VULNERABILIDADES E INFRAESTRUCTURAS CRÍTICAS

Según los expertos los problemas actuales de seguridad en la Sociedad de la Información están relacionados con la autenticación, confidencialidad, integridad y disponibilidad, de los que ya se hablarán más adelante; problemas agravados por el carácter global de la tecnología y su uso, y la ausencia de una normativa mundial y autoridad de ese ámbito. Desde esta perspectiva las legislaciones nacionales configuradas para un marco espacial-nación- limitado, resultan insuficientes para un espacio sin fronteras, lo que contribuye a aumentar los puntos vulnerables y lo que es peor, la impunidad.

66

Cuando se habla de vulnerabilidades, hay que entenderlas como la posibilidad de sufrir, en un sentido amplio, un daño: "tirar" un sistema, una intrusión, una sustracción de información... producido en las infraestructuras que soportan las comunicaciones, los sistemas de redes, las bases de datos, las aplicaciones, las herramientas... Cada día aparecen entre dos y cinco nuevas vulnerabilidades. Esto desencadena una inestabilidad y un proceso de reconfiguración vertiginoso y constante ya que los sistemas de protección diseñados para unas determinadas condiciones cuando cambian se hacen, en mayor o menor grado, ineficaces y vulnerables, por lo que hay que volver a configurarlos. Además hay que tener presente que muchas de las vulnerabilidades que se detectan son difundidas con rapidez y profusión por la red, lo que aumenta las probabilidades de nuevos y múltiples ataques. En todo caso la inmediatez, tanto en la detección como en la respuesta, es fundamental. En este sentido conviene conocer, por ejemplo, que en la base de datos SIPS (Security Intelligence Products and Systems) existe, actualmente, información de más de 101.000 ataques informáticos y 6.100 grupos de hackers. (octubre 2002) y de que la mayoría de los ataques a la seguridad de las redes corporativas aprovechan algunas de las 6.000 vulnerabilidades conocidas. Dentro de este contexto conviene recordar que las empresas e instituciones rara vez hacen público los incidentes de los que son víctimas, para no generar inseguridad e identificar y difundir sus puntos débiles, lo que lleva a pensar en la existencia de una cifra negra de delitos relacionados con el uso de las nuevas tecnologías.



Las vulnerabilidades afectan por igual a todos - instituciones, empresas y particulares- sin embargo, las consecuencias varían. No causa el mismo daño una intrusión en un ordenador personal que en una empresa u organización.

Dentro de este contexto y niveles de gravedad, los Estados, por ejemplo, dependen de una red de infraestructuras complejas, físicas y computerizadas que proporcionan servicios esenciales: energía, transporte, comunicaciones, seguridad, sistema financieros, salud, emergencias... calificados como esenciales para el funcionamiento del propio Estado, por eso se les incluye dentro de lo que se viene a denominar "infraestructuras críticas". Estas infraestructuras se encuentran en manos del sector privado, así en Estados Unidos cerca del 85% de ellas son controladas por industrias privadas y otras organizaciones no gubernamentales. Su interrupción o destrucción tendría un impacto muy grave en el bienestar, en la economía y en el funcionamiento eficaz del propio Estado. Recordemos los apagones recientes en Estados Unidos e Italia. El primero de ellos afectó a unos 50 millones de personas, se declaró el estado de emergencia, se pararon trenes, se interrumpieron los suministros de agua, se colapsaron los sistemas de telefonía móvil e Internet, etc... En un principio se atribuyó el desastre a un virus. La tendencia actual se dirige a aumentar el número de infraestructuras críticas como consecuencia de la conectividad, la interdependencia entre empresas y su creciente necesidad de las tecnologías, tomemos de nuevo como ejemplo el apagón anterior. Todas estas circunstancias incrementan la vulnerabilidades de los Estados.

67

Desde el punto de vista normativo la criminalidad informática hay que integrarla en el contexto de la "sociedad del riesgo" y precisa una regulación en ámbitos diferentes, una reforma del proceso penal para su adecuación y adaptación a estos nuevos medios, y una legislación internacional para una persecución y enjuiciamiento de este tipo de delitos que permita extender sus efectos más allá de las fronteras de los Estados. Actualmente el entramado normativo que regula la Sociedad de la Información o que está relacionada con ella, lo integran entre otras la ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico; la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y el Código Penal.

Dentro de este apartado normativo, conviene ir familiarizándose con términos como info-penas, o quizá podríamos denominarlas ciberpenas, tales como la exclusión temporal, la televigilancia, la suspensión de derechos...

También existe una preocupación creciente por la vulneración de la privacidad y la intimidad. Por ejemplo, los «cookies», ficheros que revelan los sitios web por donde ha pasado el usuario del ordenador, pueden ser

utilizados para obtener información de todo tipo. Algunas estimaciones señalan que el 92% de los sitios web de Estados Unidos recogen los datos personales de los usuarios que se suelen utilizar sin su conocimiento.

## CIBERAMENAZAS

Generalizando se puede definir la amenaza cibernética como "cualquier acción u omisión que pueda dañar, en el sentido más amplio, los sistemas de información y comunicación de las instituciones, empresas o particulares". Una característica esencial de la amenaza cibernética es su carácter anónimo. Anonimato que se potencia o refuerza en la medida que puede venir de cualquier lugar del mundo.

Las amenazas pueden ser generadas por piratas informáticos o "hackers", empleados descontentos, espionaje industrial, espionaje exterior, ataques auspiciados por otros Estados, organizaciones terroristas o delincuencia organizada, entre otros.

68

En relación con los ataques por otros Estados, la agencia Reuters difundió recientemente una noticia en la que informaba de que Corea del Norte "entrenaba alrededor de 100 cibernautas cada año para aumentar sus capacidades y poder librar una guerra cibernética, lo que obligaba a Corea del Sur a fortificar su propia seguridad informática". Corea del Sur es una de las naciones con más conexiones a Internet del mundo, lo que aumenta su vulnerabilidad. Los usuarios autorizados y, más concretamente, los trabajadores descontentos, representan la mayor amenaza para la seguridad informática de las empresas por encima de los "piratas", según un estudio realizado por el gabinete Digital Research.

Respecto al ciberterrorismo, expertos de la CIA advierten que los futuros enemigos no atacarán con armas nucleares sino penetrando en los sistemas informáticos para debilitar el potencial militar y económico. Comienza a hablarse de armas de interrupción masiva de ciberservicios. Hasta el día de hoy no hay noticias oficiales de ningún ataque que merezca el calificativo de "ciberterrorismo". Hay que aclarar que una cosa es la utilización de Internet como medio de comunicación entre los miembros de una organización terrorista y otra el ciberterrorismo. Este suele definirse por los expertos como "los ataques o intrusiones contra ordenadores o redes informáticas con el fin de intimidar, extorsionar o dañar a algún gobierno para reivindicar ideales políticos, religiosos o sociales". Por otro lado un informe del Centro para el Estudio del Terrorismo y la Guerra Irregular, de la Naval Postgraduate School en Monterrey, California señala tres niveles distintos de ciberterrorismo:

- El producido por piratas individuales que vulneran sistemas simples.



- Los ataques más complejos contra sistemas múltiples o redes.
- El tercer nivel en el que los hackers o "piratas" coordinan ataques contra redes para provocar una interrupción masiva de los servicios de Internet.

A su vez el citado estudio menciona cinco tipos de terroristas que usan los ordenadores para cometer sus atentados: religiosos, grupos de la nueva ola (ecologistas radicales, por ejemplo), etno-nacionalistas-separatistas, revolucionarios y organizaciones de extrema derecha. Por ahora, parece que sólo los grupos terroristas religiosos tienen capacidad para la ciber guerra.

En general, entre los principales tipos de amenazas que se ciernen sobre las redes de comunicación se encuentran: la denegación de servicio, interceptación de las comunicaciones, acceso no autorizado a ordenadores y redes -intrusión-, perturbación de las mismas, ataques contra los servidores de dominio, contra el sistema de encaminamiento, por saturación y denegación de servicio, ejecución de programas malintencionados que modifican y destruyen los datos como son los virus -por ejemplo el "viernes 13", "caballos de Troya", "gusanos"...- Los virus son "programas diseñados principalmente para afectar, infectar los recursos e información de sistemas informáticos aprovechando las vulnerabilidades de los mismos".

69

## SEGURIDAD EN LAS REDES

En relación con la seguridad de las redes la Comunicación 9727/01 de la Comisión a las distintas Instituciones de la Unión Europea informa que "Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos. Están compuestas de elementos de transmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y de servicios de apoyo (sistema de nombres de dominio, incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.). Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc) y de equipos terminales (teléfonos, ordenadores centrales, ordenadores personales, teléfonos móviles, organizadores personales, aparatos electrodomésticos, máquinas industriales, etc.)." y define la seguridad de esas redes como la "capacidad para resistir todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles".

Para que las redes sean seguras deben de reunir o presentar las siguientes características o requisitos:

- Disponibilidad. Significa que los datos sean accesibles y los servicios operativos, aún en caso de alteraciones del tipo de cortes de corriente, catástrofes naturales, accidentes o ataques.

- Autenticación. Confirmación de la identidad declarada de usuarios o entidades jurídicas. Hasta ahora la autenticación de una persona se basaba en la exhibición de un documento, por excelencia el de identidad y la presencia física.

En el espacio virtual esa presencia física no existe, lo que plantea un grave problema. Aunque se han puesto en marcha distintas iniciativas como la firma digital o los certificados digitales, podemos decir que nos encontramos en una fase parecida a la que se encontraban nuestros antepasados cuando buscaban un medio infalible de identificación, hasta que encontraron la impresión digital o actualmente el ADN. En este sentido tendremos que buscar una solución que sin duda llegará y será propia de la sociedad tecnológica.

- Integridad. Confirmación de que los datos que han sido enviados, recibidos o almacenados son los originales, completos y sin modificación o manipulación.

- Confidencialidad. Para impedir la interceptación y la lectura de datos.

Estas características, ya conocidas y exigidas desde siempre, deben configurarse y adaptarse a este un nuevo tipo de sociedad.

## PROTECCIÓN, DETECCIÓN Y RESPUESTA

Contextualizado el ciber-espacio y conocidas sus implicaciones, repercusiones, vulnerabilidades y amenazas, se hace necesario organizar la respuesta para un entorno que, como se comentó con anterioridad, no es geográfico y donde el tiempo adquiere una nueva dimensión, se reduce significativamente. Para este entorno la protección, detección y respuesta pasa por la prevención, la inteligencia y la colaboración a nivel nacional e internacional y no sólo entre instituciones, sino también entre las distintas y variadas organizaciones que integran la sociedad civil, es más, el simple usuario, adquiere un protagonismo especial en la detección y en la prevención. Como ya se dijo, el espacio virtual se encuentra en un proceso continuo de evolución, readaptación y utilización, por ello las tareas de inteligencia -ciber-inteligencia- adquieren una importancia crucial. La ciber-inteligencia debe de ir orientada a la captación y análisis de la infor-



mación para entender los escenarios presentes y futuros, identificar amenazas y vulnerabilidades y organizar la respuesta, todo ello desde una perspectiva transversal y estratégica.

La sensibilización es otra herramienta de respuesta a fortalecer y desarrollar. Hay que generar, como algunas asociaciones ya lo están haciendo, una cultura de seguridad. Hoy día cualquier persona que pasea por la calle o circula en vehículo adopta una serie de medidas preventivas, casi de forma instintiva y mecánica, sin embargo, en el espacio virtual, la conciencia preventiva no se ha formado, no se percibe el peligro ni el daño.

Por otra parte la información entre instituciones y sociedad civil tiene que ser fluida. Se hace absolutamente necesario compartir los conocimientos. Hay que buscar alianzas en todos los sectores, recordemos de nuevo el carácter transversal y reticular de Internet. Cualquier internauta puede ser un excelente "vigilante", esto sin contar con la multitud de asociaciones, ONG,s, que denuncian sistemáticamente conductas relacionadas con la pornografía infantil, por ejemplo, y no digamos de la disposición a colaborar de las empresas, hoy día el funcionamiento de todas o casi todas depende absolutamente de sus sistemas informáticos y de comunicaciones. Colaboración que se ve abonada por la predisposición de los usuarios de Internet. Como ejemplo de colaboración se encuentran los Centros de Alerta Temprana cuya actividad es recoger información de campo, analizarla y prevenir un hipotético desastre antes de que éste ocurra. Pese a todo, hay que seguir avanzando para mejorar la eficacia de la respuesta y por ello se hace imprescindible, además de lo expuesto anteriormente, progresar en cuestiones normativas de carácter internacional, en la formación continuada de los policías y en poner a su disposición la tecnología necesaria.

## BIBLIOGRAFÍA

– "Presente y futuro de la Seguridad en la Sociedad de la Información". Seminario. El Escorial 2000.

– "Encuesta a hogares españoles sobre tecnologías de la información y la comunicación. Informe definitivo (mayo de 2003)". Comisión del Mercado de las Telecomunicaciones.

[http://www.cmt.es/cmt/centro\\_info/publicaciones/index.htm](http://www.cmt.es/cmt/centro_info/publicaciones/index.htm)

– "Material de referencia: Resoluciones de la Asamblea General de la ONU y de la UIT."

[http://www.itu.int/wsis/documents/background.asp?lang=es&c\\_type=res](http://www.itu.int/wsis/documents/background.asp?lang=es&c_type=res)

– Oficina de Protección de Infraestructuras Críticas. Canadá.

[http://www.ociepc-bpiepc.gc.ca/critical/index\\_e.asp](http://www.ociepc-bpiepc.gc.ca/critical/index_e.asp)

– "Information insecurity"

[http://www.itu.int/wsis/docs/background/themes/security/information\\_insecurity\\_2ed.pdf](http://www.itu.int/wsis/docs/background/themes/security/information_insecurity_2ed.pdf)

72

– "Indicadores de la Sociedad de la Información en España y varios países de la OCDE 1995-2003".

<http://www6.mcyt.es/indicadores/>

– "eEurope 2005: Una sociedad de la información para todos"

[http://www.cdsi.es/documentos/eeurope\\_2005\\_action\\_plan.pdf](http://www.cdsi.es/documentos/eeurope_2005_action_plan.pdf)

– Documentos. Comisión de Estudios para el Desarrollo de la Sociedad de la Información.

<http://www.cdsi.es/documentos.htm>

– "La amenaza cibernética: la protección de las redes de información estadounidenses."

<http://usinfo.state.gov/journals/itps/1198/ijps/ijps1198.htm>

– Delitos informáticos.

<http://delitosinformaticos.com/noticias/99310916041749.shtml>

– Seguridad en la red

([www.segured.com](http://www.segured.com))



## **NORMATIVA ESPAÑOLA Y COMUNITARIA**

**Noelia García Noguera**  
**Abogada. Especialista en Nuevas Tecnologías**

Esta conferencia es un recorrido por la legislación española y comunitaria que enmarca normativamente a la Sociedad de la Información. El camino se inicia con los contenidos de una Ley específica para el desarrollo de esa sociedad, continúa con la de Protección de Datos y concluye con los tipos penales más representativos y las Directivas de la Unión Europea.

73

### **LEY 34/2002, DE 11 DE JULIO, DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO. (LSSI)**

El principal objetivo de la Ley es la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior. Además, también tiene como objetivo incorporar parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores y, especialmente, la acción de cesación.

En la Ley se parte de un concepto amplio de “servicios de la sociedad de la información”.

Este concepto engloba los siguientes campos:

- La contratación de bienes y servicios por vía electrónica.
- El suministro electrónico de información.
- Las actividades de intermediación relativas a la provisión de acceso a la red.

- La transmisión de datos por redes de telecomunicaciones.
- La realización de copia temporal de las páginas de Internet solicitadas por los usuarios.
- El alojamiento de información en servidores.
- Los servicios o aplicaciones facilitadas por otros.
- Provisión de instrumentos de búsqueda o de enlaces.
- Cualquier otro servicio o aplicación facilitado a petición individual de los usuarios.

En general, todas estas actividades descritas serán prestadas por los siguientes agentes:

- Operadores de telecomunicaciones.
- Proveedores de acceso a Internet.
- Portales.
- Motores de búsqueda.
- Cualquier sujeto que disponga de un sitio en Internet en el que realice alguna de las actividades señaladas, incluido el comercio electrónico.

74

La Ley se aplica a los prestadores establecidos en España. Además, también se aplica a los no residentes en España pero que cuenten en nuestro país con un establecimiento permanente.

## OBJETO

Es “la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica”, todo ello sin perjuicio de lo que se disponga en otro tipo de leyes estatales o autonómicas.

### **¿Qué se entiende por servicios de la sociedad de la información?**

Se establece que será todo servicio prestado:

- Generalmente a título oneroso.
- A distancia.
- Por vía electrónica.
- A petición del destinatario.



No obstante, también se establece que podrán incluirse en este concepto servicios no remunerados, siempre que constituyan una actividad económica para el prestador del servicio.

## **OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN**

Las principales obligaciones de los prestadores de servicios de la sociedad de la información son las siguientes:

### **Constancia registral del nombre de dominio**

Los prestadores de servicios deberán comunicar al Registro Mercantil en el que se encuentren inscritos, un nombre de dominio, así como todo acto de sustitución o cancelación del mismo, en el plazo de un mes desde la obtención, sustitución o cancelación del mismo. Esta comunicación posee efectos meramente publicitarios. En caso de que se utilicen nombres de dominio antes de la entrada en vigor de esta Ley, tendrán de plazo hasta el 12 de octubre del 2003.

### **Información general**

Los prestadores de servicios deberán facilitar a los usuarios, de una forma fácil, directa y gratuita, las siguientes informaciones:

- Su nombre o denominación social.
- Su residencia, domicilio o dirección de uno de sus establecimientos permanentes
- Su dirección de correo electrónico.
- Los datos de inscripción en el Registro.
- Los datos de la autorización administrativa y del órgano encargada de su supervisión, en su caso.
- Los datos del Colegio Profesional y el número de colegiado, en su caso.
- El NIF
- Información clara y exacta sobre el precio de los productos o servicios, indicando si incluyen o no los impuestos y los gastos de envío, en su caso.
- Los códigos de conducta a los que se adhiera y la manera de consultarlos.

## **Deber de colaboración**

Los prestadores de servicios de intermediación deberán colaborar para que se interrumpa la prestación de un servicio en caso de que un órgano competente se lo ordene (judicial o administrativo).

## **Deber de retención de datos de tráfico relativos a las comunicaciones electrónicas:**

Los operadores de redes, los proveedores de accesos y los prestadores de servicio de alojamiento deberán retener este tipo de datos por un período máximo de 12 meses.

Los datos que deben almacenar serán aquellos que identifiquen el origen de los datos alojados y el momento en que se inició la prestación del servicio y respetando, en todo momento, el secreto de las comunicaciones.

La finalidad de estos datos albergados será su conservación para una futura utilización en el marco de una investigación criminal, la salvaguarda de la seguridad pública y la defensa nacional. Los obligados a conservar estos datos no los podrán utilizar para otra finalidad.

76 En esta materia se prevé un desarrollo reglamentario que especifique mejor esta obligación.

## **RÉGIMEN DE RESPONSABILIDAD**

En primer lugar hemos de señalar que todo tipo de prestadores de servicios de la sociedad de la información están sujetos a responsabilidad civil, penal y administrativa. Respecto a la responsabilidad de los prestadores de servicios de intermediación se seguirán las siguientes normas:

### **Operadores de redes y proveedores de acceso**

No serán responsables de la información que transmitan a no ser que originen la transmisión, modifiquen los datos o seleccionen los datos o a sus destinatarios.

Los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios no serán responsables del contenido de los datos ni de la reproducción temporal de los mismos siempre que:

- No modifiquen la información.
- Permitan el acceso sólo a los destinatarios que cumplen con los requisitos impuestos por el destinatario cuya información se solicita.
- Respeten las normas generalmente aceptadas por el sector.

- No interfieran en la utilización lícita de tecnología generalmente aceptada por el sector.
- Retiren la información que hayan almacenado o no permitan el acceso a ello cuando tengan el conocimiento efectivo de:
  - Que esta información ha sido retirada del lugar de la red en que se encontraba inicialmente.
  - Que se ha imposibilitado el acceso a ella.
  - Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir su acceso.

### **Prestadores de servicios de alojamiento o almacenamiento de datos**

Serán responsables de la información almacenada a petición del destinatario, siempre que tengan conocimiento de que la actividad o la información es ilícita o “de que lesiona bienes o derechos de un tercero susceptibles de indemnización” y no actúen “con la diligencia debida para retirar los datos o hacer imposible el acceso a ellos”.

### **Prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda**

Serán responsables de la información que faciliten o de los instrumentos de búsqueda, siempre y cuando tengan conocimiento de que la actividad o la información a la que remiten o recomiendan es ilícita o “de que lesiona bienes o derechos de un tercero susceptibles de indemnización” y no actúen “con la diligencia debida para retirar los datos o hacer imposible el acceso a ellos”.

77

## **COMUNICACIONES COMERCIALES**

El régimen jurídico de las comunicaciones comerciales es el siguiente:

- La propia Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- La normativa propia en materia comercial y de publicidad.
- La Ley Orgánica de Protección de Datos.

Como principio general se establece la prohibición de envío de comunicaciones publicitarias o promocionales, si previamente el interesado no hubiera solicitado expresamente su envío. En caso de autorizarse, el interesado puede revocar en cualquier momento su consentimiento.

Cuando se autoricen estas comunicaciones comerciales, deben cumplir una serie de requisitos:



- Deben estar claramente identificadas y al comienzo del mensaje deben incluir la palabra "publicidad".
- Deben indicar a la persona, física o jurídica, en nombre de la cual se realizan.
- En caso que se recabe la dirección de correo electrónico de una persona, en un proceso de contratación on line, y se desee utilizar para el envío de comunicaciones comerciales, antes de terminar el procedimiento de contratación, se debe informar a esa persona de la intención de utilizar su dirección de correo para este fin, así como, se debe solicitar su consentimiento para la recepción de estas comunicaciones.
- Deben establecer mecanismos sencillos y gratuitos para que el interesado pueda revocar su consentimiento de recibir comunicaciones comerciales.
- Deben facilitar la información sobre los procedimientos de revocación del consentimiento.
- En el supuesto de ofertas promocionales, se deberán indicar que se trata de una oferta de este tipo y deberán recogerse "de forma clara e inequívoca" las condiciones de acceso y de participación a las mismas.

## CONTRATACIÓN ELECTRONICA

La Ley otorga plena validez y eficacia a los contratos celebrados de forma electrónica, siempre y cuando respeten las condiciones generales de validez recogidas en el Código Civil, el Código de Comercio, las normas de protección de consumidores y usuarios, las normas de ordenación de la actividad comercial y las demás reguladoras civiles y mercantiles referentes a los contratos.

Por otro lado, cuando una norma exija que un contrato o cualquier información que se relaciona con él deba constar por escrito, ésta exigencia se entenderá cumplida si el contrato o alguna de sus informaciones se recogen en un soporte electrónico.

La prueba de los contratos electrónicos se atenderá a lo dispuesto en la legislación sobre firma electrónica. Además, el soporte electrónico en el que conste un contrato, se deberá admitir como prueba documental en juicio.

En cuanto al lugar de celebración del contrato, éste se presumirá celebrado en el lugar de residencia del consumidor (claro está cuando se trate de contratos celebrados con consumidores).

En los contratos celebrados entre "empresarios o profesionales", el

contrato se presumirá celebrado en el lugar que se encuentre establecido el prestador de servicios, en defecto de acuerdo entre las partes.

En el caso de contratos celebrados con consumidores previamente a la celebración de un contrato electrónico, se deberán cumplir los siguientes requisitos:

- 1.- Informar de manera “clara, comprensible e inequívoca” de las siguientes cuestiones:
  - Los pasos que deben seguirse para la contratación electrónica.
  - Si se va archivar el documento electrónico en el que se formalice el contrato y si tal documento va a poder ser accesible.
  - Los medios técnicos que el consumidor dispone para identificar y corregir errores en la introducción de datos.
  - La lengua o lenguas en que se puede formalizar el contrato.
- 2.- Poner a disposición de los consumidores las condiciones generales de la contratación. Éstas tienen que poder almacenarse y reproducirse por el consumidor. Esta obligación es genérica para todo tipo de procesos de contratación electrónica, no sólo cuando el destinatario sea un consumidor.

79

El primer requisito (información previa) no será necesario cuando ambas partes así lo acuerden (y siempre y cuando una de ellas no sea consumidor) o cuando se celebre el contrato mediante el intercambio de correos electrónicos “cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento” de esta obligación.

Además de estos requisitos previos al inicio del procedimiento de contratación, y siempre que se trate de contratos celebrados con consumidores, se exige posteriormente que el prestador de servicios confirme la aceptación del consumidor. La Ley establece dos medios para confirmar esta recepción:

- Envío de acuse de recibo por correo electrónico en 24 horas desde que se recibió la aceptación.
- Confirmación por un medio equivalente al seguido en el procedimiento de contratación, siempre que esta confirmación pueda ser archivada por el consumidor.

## SOLUCIÓN JUDICIAL Y EXTRAJUDICIAL DE CONFLICTOS

### **Acción de cesación**

Esta acción podrá ejercerse por las personas legitimadas y conforme a lo dispuesto en la Ley de Enjuiciamiento Civil, contra las conductas contrarias a esta Ley que “lesionen intereses colectivos o difusos de los consumidores”

Se encuentran legitimados para interponer esta acción:

- Las personas físicas o jurídicas con intereses o derechos legítimos.
- Los grupos de consumidores o usuarios según lo dispuesto en la Ley de Enjuiciamiento Civil.
- Las asociaciones de consumidores y usuarios que reúnan los requisitos establecidos en la legislación de defensa de los consumidores.
- El Instituto Nacional de Consumo y sus análogos autonómicos y locales.
- El Ministerio Fiscal.
- Las entidades de Estados miembros de la UE habilitadas para tal fin.

80

### **Solución extrajudicial**

Se prevé que los conflictos que puedan surgir se resuelvan a través de los arbitrajes establecidos en la legislación de arbitraje y de defensa de consumidores y usuarios o los que se recojan en los Códigos de Conducta.

## INFRACCIONES Y SANCIONES

La persona encargada de la imposición de sanciones por infracciones muy graves será el Ministro de Ciencia y Tecnología, mientras que el competente para la imposición de sanciones por infracciones graves y leves será el Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, sin perjuicio de la competencia que pudieran tener otros órganos administrativos por el incumplimiento de las resoluciones dictadas por estos órganos relativas a la restricción de la libre competencia o relativas al deber de colaboración.



En todo caso se atenderá a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo.

## INFRACCIONES LEVES

Se consideran infracciones leves las siguientes:

- La no comunicación a los Registros pertinentes del nombre de dominio.
- No informar a los usuarios sobre:
- Los datos de inscripción en el Registro.
- Los datos de la autorización administrativa y del órgano encargado de su supervisión, en su caso.
- Los datos del Colegio Profesional y el número de colegiado, en su caso.
- El NIE.
- Los códigos de conducta a los que se adhiera y la manera de consultarlos.
- No cumplir con los requisitos relativos a las comunicaciones comerciales, cuando este incumplimiento no suponga otra infracción más grave.
- Incumplir los requisitos previos al inicio del procedimiento de contratación electrónica, cuando este incumplimiento no suponga una infracción más grave.
- Incumplir el requisito de confirmación de la recepción de la aceptación del consumidor en el procedimiento de contratación electrónica, cuando este incumplimiento no suponga una infracción más grave.

Las infracciones señaladas pueden llevar consigo las siguientes sanciones:

- Una multa de hasta 30.000 euros.
- El impedimento de acceso desde España a los servicios ofrecidos, cuando se trate de prestadores de la UE o del EEE, durante un plazo máximo de hasta 6 meses.
- La prescripción de las infracciones leves será de seis meses y la de las sanciones impuestas a este tipo de infracciones será de un año.

## INFRACCIONES GRAVES

Se consideran infracciones graves las siguientes:

- No informar a los usuarios sobre:
  - El nombre o denominación social.
  - La residencia, domicilio o dirección de uno de los establecimientos permanentes.
  - La dirección de correo electrónico.
  - El precio de los productos o servicios, indicando si se incluyen o no los impuestos y los gastos de envío, en su caso.
- El envío masivo de comunicaciones comerciales a destinatarios que no hayan solicitado o autorizado expresamente su remisión.
- El envío, en el plazo de un año, de más de tres comunicaciones comerciales a un mismo destinatario, cuando éste no hubiera solicitado o autorizado su remisión.
- No poner a disposición de los usuarios las condiciones generales, en el procedimiento de contratación electrónica.
- El incumplimiento habitual del requisito de confirmación de la recepción de la aceptación del consumidor, en el procedimiento de contratación electrónica.
- La resistencia, excusa o negativa a la actuación inspectora de los órganos facultados.

82

Las infracciones especificadas pueden llevar consigo las siguientes sanciones:

- Una multa de 30.001 a 150.000 euros.
- La publicación, a costa del sancionado de la sanción en los Boletines Oficiales correspondientes, en dos periódicos de difusión pertinente o en la página de inicio del prestador de servicios.
- El impedimento de acceso desde España a los servicios ofrecidos, cuando se trate de prestadores de la UE o del EEE, durante un plazo máximo de hasta un año.
- La prescripción de las infracciones graves, así como de las sanciones impuestas a este tipo de infracciones será de dos años.

## INFRACCIONES MUY GRAVES

Se considerarán infracciones muy graves las siguientes:

- El incumplimiento de las órdenes dictadas relativas a la restricción de la libre competencia.
- El incumplimiento de las órdenes dictadas relativas al deber de colaboración.
- El incumplimiento del deber de retención de datos de tráfico relativos a las comunicaciones electrónicas.
- La utilización de los datos que deben ser retenidos, en virtud del deber de retención de datos de tráfico relativos a las comunicaciones electrónicas, para fines distintos a los establecidos.

Estas infracciones pueden llevar consigo las siguientes sanciones:

Una multa de 150.001 a 600.000 euros.

La publicación, a costa del sancionado de la sanción en los Boletines Oficiales correspondientes, en dos periódicos de difusión pertinente o en la página de inicio del prestador de servicios.

El impedimento de acceso desde España a los servicios ofrecidos, cuando se trate de prestadores de la UE o del EEE, durante un plazo máximo de hasta dos años.

Cuando se produzca, en el plazo de tres años, una reiteración de dos o más infracciones muy graves, sancionadas con carácter firme, se podrá sancionar, además con la prohibición de actuación en España durante un plazo máximo de dos años.

La prescripción de las infracciones muy graves, así como de las sanciones impuestas a este tipo de infracciones será de tres años.

## MEDIDAS PROVISIONALES Y MULTA COERCITIVA

En los procedimientos sancionadores, e incluso antes de su iniciación, siempre que existan motivos de urgencia y de protección de los intereses implicados, se podrán adoptar medidas provisionales para "asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales".



Las medidas provisionales que se podrán acordar podrán ser las siguientes:

- Suspensión temporal de la actividad del prestador de servicios.
- El cierre temporal del prestador de servicios.
- El precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos, aparatos y equipos informáticos del prestador de servicios.
- La advertencia al público de la posible existencia de conductas infractoras.

El órgano administrativo competente, podrá acordar la imposición de una multa coercitiva de hasta 6.000 euros diarios, en caso de no cumplimiento de las medidas provisionales descritas.

## **LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

### **Legislación Estatal Española**

84

- L.O. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.

- Real Decreto 1332/1994, de 20 de Junio, por el que se desarrolla determinados aspectos de la LORTAD.

### **Legislación europea**

- Directiva 95/46/CE del Parlamento Europeo y el Consejo de la Unión Europea.

### **Legislación comunidad autónoma de Madrid**

- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid.

- Ley 13/1995, de 21 de abril, de regulación del uso de informática en el tratamiento de datos personales por la Comunidad de Madrid. B.O.C.M. n° 105, de 4 de mayo de 1995.

- Decreto 22/1998, de 12 de febrero, por el que se aprueba el Estatuto de la Agencia de Protección de Datos de la Comunidad de Madrid.
- R.D. 26-03-1993, Estatuto de la Agencia de Protección de Datos.

## INTRODUCCIÓN

El derecho a la protección de datos personales tiene antecedentes importantes en el ámbito europeo, como el Convenio de 28 de Enero de 1981 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y el Acuerdo de Schengen de 14 de Junio de 1985.

En España, en virtud del artículo 18.4 de la CE, que limita el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos, se elaboró la LORTAD (Ley Orgánica 5/92, Reguladora del Tratamiento Automatizado de Datos).

Esta norma nació en cumplimiento de la obligación de España de adoptar, antes de la ratificación del Acuerdo de Schengen, todas las iniciativas necesarias para adaptar el ordenamiento interno español a las exigencias del Convenio 108 del Consejo de Europa para la protección de las personas en lo relativo al tratamiento automatizado de los datos de carácter personal.

El siguiente paso fue la aprobación de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, en adelante LOPD, en desarrollo del mandato contenido en la Directiva 95/46/CE que obligaba a los Estados miembro a adoptar las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la Directiva en un período máximo de tres años.

La LOPD, se aplica a los datos de carácter personal<sup>(1)</sup> registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Los ficheros automatizados creados con anterioridad al 14 de enero del 2000 (fecha de entrada en vigor de la LOPD), deberían haberse adecuado a la LOPD antes del 14 de enero del 2003.

Los ficheros no automatizados deben adaptarse a la LOPD antes del 24 de octubre del 2007.

---

1.- "dato de carácter personal": cualquier información concerniente a personas físicas identificadas o identificables.

## PRINCIPIOS DE LA PROTECCIÓN DE DATOS

### Calidad de los datos

Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Estos condicionantes han de ponerse en relación con el caso en concreto.

### Finalidad

Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para la que se hubieran recogido. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

Los datos de carácter personal incorporados al fichero han de responder a la situación actual, de manera que recojan todas las modificaciones surgidas, y una vez incorporadas responderán a la realidad.

86 Así mismo, los datos de carácter personal han de ser exactos, de manera que si resultan ser inexactos o incompletos, en todo o en parte, han de ser cancelados o sustituidos de oficio por el responsable del fichero.

Cuando se ha cumplido la finalidad para la que se recabaron los datos han de ser cancelados o destruidos, en caso de no ser posible han de ser bloqueados.

### Información

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- a) De que sus datos van a ser incluidos en un fichero, de la finalidad de la recogida y de los destinatarios de la información.
- b) De la obligatoriedad o no de dar esos datos.
- c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- d) De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.
- e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante para que los afectados puedan ejercer sus derechos.



Todas estas advertencias deberán ser recogidas en aquellos cuestionarios e impresos utilizados para la recogida de los datos.

No será necesaria la información a que se refieren los puntos b), c) y d) si el contenido de ellas se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. Las empresas no necesitan pedir a sus empleados cada mes los datos necesarios para realizar las nóminas, ya que hay una relación laboral.

### **Consentimiento**

La LOPD establece que el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco, es decir, expreso o tácito, del afectado, salvo que la ley disponga otra cosa. El artículo 7.2 de este mismo texto legal exige para los datos especialmente protegidos consentimiento expreso y por escrito dada la importancia de los mismos.

No será preciso el consentimiento:

- Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.
- Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- Cuando el tratamiento de datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7.6 de la presente Ley.

87

En estos casos en los que no es necesario el consentimiento del afectado, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

### **Seguridad de los datos**

El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

### **Deber de secreto**

Tanto el responsable del fichero, como el encargado de tratamiento, así como cualquier persona que intervenga en cualquier fase del proceso, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

## OBLIGACIONES LEGALES

La norma establece las siguientes obligaciones legales:

- Inscripción de los ficheros en el Registro General de la Protección de Datos. Artículo 26 LOPD. Artículos. 5 y 6 R.D. 1332/1994, de 20 de Junio.
- Redacción del documento de seguridad. "El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de seguridad de obligado cumplimiento para el personal con acceso a los datos automatizados de carácter personal y a los sistemas de información" R.D. 994/1999, de 11 de Junio.
- Redacción de cláusulas de protección de datos. Artículo 5 LOPD:
- Auditoría. Artículo 17 R.D. 994/1999, de 11 de Junio.
- Demás medidas de seguridad de índole técnica y organizativas necesarias para garantizar la seguridad de los datos objeto de tratamiento. Artículos 9 y 10 LOPD y R.D. 994/1999, de 11 de junio.
- Redacción de los contratos, formularios y cláusulas necesarias para la recogida de datos, los tratamientos por terceros y las cesiones o comunicaciones de datos.

88

## ¿QUÉ DERECHOS OTORGA LA NORMATIVA DE PROTECCIÓN DE DATOS A LOS USUARIOS?

Los principales derechos son los siguientes:

- Derecho de información. Artículo 5 LOPD.
- Necesidad de solicitud de su consentimiento. Artículo 6 LOPD.
- La impugnación de valoraciones. Artículo 13 LOPD.
- Derecho de consulta al Registro General de Protección de Datos. Artículo 14 LOPD.
- Derecho de acceso, rectificación y cancelación de datos. Artículos 15, 16 y 17 LOPD.
- Derecho de oposición. Artículo 17 LOPD.
- Tutela de los derechos. Artículo 18 LOPD.
- Derecho de indemnización. Artículo 19 LOPD

## MENCIÓN A LOS DATOS ESPECIALMENTE PROTEGIDOS. DATOS MÉDICOS

No existe una definición de datos de salud en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal (en adelante LOPD), ni en el Real Decreto 1332/1994, de 20 de Junio por el que se desarrollan determinados aspectos de la LORTAD.

Sin embargo, la Recomendación nº (97)5 de 13 de Febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembro sobre Protección de Datos Médicos, da una definición general de "dato médico" definiéndolo como todo dato personal relativo a la salud de un individuo, incluyendo aquellos que tienen una clara y estrecha relación.

Los datos relativos a la salud tienen la consideración de datos especialmente protegidos, y la razón de ello reside en que forman parte de la intimidad y privacidad del individuo, derecho reconocido y protegido por nuestra constitución. (artículo 18.1 y 4 C.E.)

El párrafo 3 del artículo 7 de la LOPD establece que los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual solo podrán ser recabados, tratados y cedidos cuando por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

El artículo 8 de la LOPD, establece específicamente para los datos relativos a la salud lo siguiente:

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

De manera que serán los profesionales sanitarios o los individuos u órganos que trabajen en representación de los mismos los únicos legitimados para recoger y procesar datos médicos.

Cuando un paciente da sus datos a un profesional sanitario para que éste forme su ficha médica o en caso de ingreso hospitalario, puede exigir al médico que le informe sobre que va a pasar con esos datos. El paciente debe ser informado de modo expreso, preciso e inequívoco que sus datos van a ser recogidos en un fichero, de la finalidad de la recogida y de los destinatarios de los mismos.



Así mismo, el paciente puede ejercitar los derechos de acceso, rectificación, cancelación y oposición, y para ello deberá ser informado de la identidad del responsable del tratamiento y de la dirección del mismo.

## **DELITOS VINCULADOS O RELACIONADOS CON LAS NUEVAS TECNOLOGÍAS**

### **DELITO DE ESTAFA INFORMÁTICA (Art. 248.2 C.P. Español):**

Los principales elementos que integran genéricamente el delito de estafa son:

- El ánimo de lucro.
- La acción típica es la de valerse de una manipulación informática o artificio semejante.
- La transferencia no consentida del patrimonio de otra persona sin utilizar violencia.
- Perjuicio a tercero.

### **90 Los fraudes más comunes en Internet:**

- Las subastas: algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos. Una vez que el consumidor ha enviado el dinero puede ocurrir que reciban algo con menor valor de lo que creían, o peor todavía, que no reciban nada.

- Las tarjetas de crédito: en algunos sitios de Internet, especialmente para adultos, se pide el número de la tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años. El verdadero objetivo es cobrar cargos no solicitados.

- Ventas piramidales: consiste en ofrecer a los usuarios falsas promesas de ganar dinero de manera fácil sólo por vender determinados productos a nuevos compradores que éstos deben buscar.

- Viajes y vacaciones: determinadas páginas de Internet ofrecen destinos maravillosos de vacaciones a precios de ganga, que a menudo encubren una realidad completamente diferente o inexistente.

- Oportunidades de negocio: convertirse en jefe de uno mismo y ganar mucho dinero es el sueño de cualquiera. En la Red abundan las ofertas para ganar fortunas invirtiendo en una aparente oportunidad de negocio que acaba convirtiéndose en una estafa.

- Inversiones: las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y comportan grandes

riesgos para los usuarios. Como norma general, no es recomendable fiarse de las páginas que garantizan inversiones con seguridad del 100%.

- Productos y servicios milagro: algunas páginas de Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias. Hay quienes ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

Las estafas del 906 en España: falsas ofertas de trabajo, videntes, páginas web gratuitas que suponen más de 60 euros la hora de conexión a Internet, regalos que acaban costando menos que la llamada que hay que realizar para confirmarlos... Son algunos de los nueve tipos de fraudes y abusos más frecuentes a través de las líneas 906. Estos son los nueve tipos de fraudes y abusos que se producen a través de las descontroladas y sin regulación líneas 906:

- Contactos: a través de diversas páginas web se anuncian contactos entre personas, desde contactos íntimos hasta amistad y matrimonio. Una vez suscrito y tras dar una serie de datos personales como tu carácter, físico y el tipo de relación que buscas, tu anuncio es publicado. Si alguien ve el anuncio y está interesado se pone en contacto, pero para recibir su mensaje es necesario descargarse el tan conocido Dialer, que se conecta a través de un 906.

- Ofertas de trabajo: se anuncian generalmente en las páginas de ofertas de empleo de los diarios. Los teleoperadores realizan un largo cuestionario, prolongando al máximo la duración de la llamada. En ocasiones, solicitan incluso una fotografía o un currículum por escrito para dar una apariencia de credibilidad al timo. Pero en realidad, nunca se recibe respuesta ya que los trabajos no existen.

- Regalos y premios: el usuario recibe una llamada, una carta o un e-mail donde se le informa que ganado un sorteo o que una empresa ha decidido hacerle un regalo. Para más información, una línea 906. La llamada a este número puede tener varios resultados: una convocatoria a una presentación comercial donde se intentará que el usuario compre un producto, cuya asistencia es indispensable para recibir el regalo; la explicación de que el regalo consiste en varias noches en un hotel o apartamento, pero con la condición de abonar la comida o unos supuestos gastos de gestión; la confirmación de un fantástico regalo, del que únicamente habrá que pagar unos gastos de envío sospechosamente altos; e incluso un largo mensaje grabado que avisa de que todas las líneas están ocupadas.

- Videntes: los que piensan que las artes adivinatorias son un don propiedad de privilegiados están muy equivocados. Hoy en día, cualquiera puede tener estos poderes. Y es que los supuestos adivinos, astrólogos, brujos o futurólogos bendecidos por los medios de comunicación se han visto tan desbordados de llamadas que no han tenido otro remedio que contratar a equipos de adivinos para atender las consultas telefónicas. ¿Qué cua-



lidades hay que reunir para ser vidente? Capacidad para retener una llamada, inventiva y un poco de psicología barata.

- Páginas web 'gratuitas': numerosas páginas web, generalmente eróticas o pornográficas, que se anuncian como gratuitas condicionan su visionado a que el usuario instale en su ordenador un programa, ocultando o disimulando que la función del mismo es desconectar el modem para volverlo a conectar a Internet, pero a través de líneas 906. Teniendo en cuenta las elevadas tarifas de estas líneas, el internauta puede llegar a pagar hasta más de 60 euros por una hora de conexión a la red.

- Confirmaciones de pedidos: el usuario recibe un e-mail de una empresa que le anuncia que en breve le cargará en su tarjeta de crédito una cantidad en concepto de una supuesta compra que en realidad no ha realizado. La empresa facilita únicamente un teléfono 906 para solucionar las posibles dudas que tenga el cliente. Generalmente, el usuario se intenta poner en contacto con la empresa para anular el falso pedido a través de este teléfono, y en él un contestador retiene su llamada durante un largo rato, advirtiendo por ejemplo que las líneas están saturadas.

- Concursos: en muchos casos, los cada vez más frecuentes concursos de la televisión no informan del precio de la llamada o se hace en letra pequeña. La llamada también puede prolongarse debido a mensajes excesivamente largos que el usuario tiene que escuchar antes de dejar su mensaje. En muchos casos, no se informa del tiempo que estará vigente el concurso, por lo que el usuario desconoce las probabilidades que tiene de ganar un premio que, generalmente, es de una cuantía ridícula en comparación con el coste de la llamada y el número de usuarios que participan.

- Líneas eróticas: en ocasiones, lo que se presenta como una conversación erótica se reduce a una simple grabación. Asimismo, quienes atienden estos teléfonos hacen lo posible, como en el resto de líneas 906, por prolongar al máximo las llamadas.

- Consultorios: cada vez más profesionales ofrecen sus servicios a través de líneas 906. El problema es que, si bien la atención a través del teléfono deja mucho que desear en comparación de una cita en persona, el usuario no tiene generalmente forma de comprobar si la persona que está tras la línea tiene realmente la cualificación profesional que anuncia o ésta es la misma que la de los equipos de videntes que atienden otras líneas 906.



## DELITOS CONTRA LA PROPIEDAD INTELECTUAL

La normativa que protege la propiedad intelectual es la siguiente:

- Directiva 91/250/CEE del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador
- Directiva 96/9/CE del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos
- Directiva 2001/29/CE del parlamento europeo y del consejo de 22 de mayo de 2001 relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la Sociedad de la Información.
- Código Penal Español.

La violación de los derechos de autor y derechos afines debe sancionarse, al igual que la elusión de las medidas tecnológicas diseñadas para proteger estos derechos.

### Artículo 270 C.P.

Conductas típicas:

1.- Reproducir. Fijación de una obra en un medio que permita su comunicación y la obtención de copias de toda o parte de ella.

La realización de copias requiere la autorización del titular, salvo:

- Que sea para uso privado.
- Que no sea para utilización colectiva.
- Que no tenga carácter colectivo.

Los programas de ordenador están fuera de este régimen, por lo que es necesaria autorización de su titular para realizar una copia, salvo la de seguridad.

2- Distribuir. Puesta a disposición del público del original o copias de la obra mediante la venta, alquiler, préstamo o de cualquier otro modo.

3.- Transformar. La transformación de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente.

No se considera que se altera la obra cuando el usuario lo modifique para adaptarlo a sus necesidades.

4.- Comunicación Pública. Acto por el cual una pluralidad de personas tienen acceso a la misma sin previa distribución de ejemplares a las mismas.

## **DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL ESPAÑOL**

Con la expresión delito informático se define a todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

A continuación vamos a enumerar algunos de los delitos "nuevos" introducidos en el CP 1995:

### **Descubrimiento y revelación de secretos** (Artículo 197 C.P.)

"El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses".

Se trata de un delito contra la intimidad, por ello la interceptación del correo electrónico se asimila a la violación de la correspondencia.

El Código Penal no había previsto las modalidades comisivas consistentes en el uso de las tecnologías de la información para invadir la intimidad de las personas o para violar, acceder o descubrir sus secretos.

### **Hacking**

Mero acceso no consentido. Conocido como hacking directo: acceso indebido o no autorizado con el único ánimo de vulnerar el password sin ánimo delictivo adicional. No se encuentra penado en el Código Penal.

Hacking indirecto. Supone un acceso in consentido al ordenador o sistema informático como medio para cometer diferentes conductas delictivas. Se castiga por el delito finalmente cometido. (ej, daños, interceptación del correo electrónico, etc).

### **Espionaje informático empresarial** (Artículo 278 C.P.)

Aquí el bien jurídico protegido es el secreto empresarial, la información almacenada informáticamente que supone un valor económico

para la empresa porque confiere al titular una posición ventajosa en el mercado.

### **Daños informáticos o sabotaje** (Artículo 264.2 C.P.)

“... al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos”.

Se trata de los daños causados en el sistema informático mediante la introducción de virus y bombas lógicas.

En el código penal anterior sólo se preveía la destrucción de bienes materiales, por lo que los daños causados a bienes inmateriales no estaban incluidos en este delito.

### **Pornografía infantil** (Artículo 189 C.P.)

En este caso se incluye la expresión “el que por cualquier medio” con el fin de incluir Internet como medio para cometer este delito.

Delitos tradicionales existentes hasta ahora en el código penal y que son de perfecta aplicación a los cometidos por medios informáticos:

- Difusión y exhibición de material pornográfico a menores:

El artículo 186 C.P. castiga el hecho de exhibir material pornográfico a menores a través de cualquier medio, por ejemplo el correo electrónico.

### **Calumnia** (Artículos 205 y 206 C.P.)

Consiste en la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad.

### **Injuria** (Artículo 208 y 209 C.P.)

Es posible llevar a cabo estos delitos a través del correo electrónico o incluso a través de terminales móviles.

### **Calumnias e injurias hechas con publicidad** (Artículo 211 C.P.)

En este supuesto cabe perfectamente la difusión de mensajes injuriosos o calumniosos a través de Internet.

### **Delito tradicional de daños** (Artículo 263 C.P.)



## **Robo** (Artículo 237 C.P.)

Se requiere el uso de la fuerza en las cosas. El artículo 238 establece que se realiza el robo con fuerza cuando se llevan a cabo con llaves falsas, que según el artículo 239 llaves falsas son las tarjetas, y los mandos o instrumentos de apertura a distancia.

Gran parte de la doctrina que considera que no es posible el delito de robo ni de hurto de datos, porque no tienen naturaleza corpórea, tangible y no son susceptibles de aprehensión.

## **Defraudaciones de fluido eléctrico** (Artículo 255 C.P.)

“Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones (televisión, teléfono, etc) u otro elemento, energía o fluido ajenos”.

Es necesario que se ocasione un perjuicio superior a 300 Euros, si es inferior se reenvía al artículo 623 C.P (faltas contra el patrimonio)

## **Defraudación a través de equipo terminal de comunicaciones** (Artículo 256 C.P.)

Se refiere al uso no autorizado o abusivo de terminales de telecomunicaciones ocasionando un perjuicio superior a 300 Euros.

## **Delitos contra la propiedad intelectual** (Artículo 270 C.P.)

Los actos ilícitos que no cumplan con los requisitos del tipo se remiten a multa del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.

## **Delitos contra la propiedad industrial** (Artículo 273 C.P.)

### **Publicidad ilícita** (Artículo 282 C.P.)

### **Falsedad de documento público** (Artículo 390 C.P.)

### **Falsedad de documento privado** (Artículo 395 C.P.)

**ANTEPROYECTO DE LEY ORGÁNICA  
POR LA QUE SE MODIFICA LA LEY ORGÁNICA 10/1995,  
DE 23 DE NOVIEMBRE, DEL CÓDIGO PENAL**

Se introducirán catorce nuevos delitos y faltas con el fin de regular determinadas conductas delictivas no recogidas en el código penal o desarrollar su regulación actual.

Se va a introducir un nuevo delito, que castigará la fabricación, introducción, posesión o facilitación de programas de ordenador para cometer estafas. Aquí se incluiría la estafa llevada a cabo a través de las líneas 906 y los ya famosos Dialer.

Se incluye como delito la conducta de utilizar sin autorización equipos y programas para acceder a radios y televisiones de pago o a servicios prestados vía electrónica, denominado "Fraude en el acceso condicionado a telecomunicaciones".

Se pretende unificar la definición del delito de fraude en toda la UE e incluir dicho concepto en la futura Ley sobre la Orden Europea de Detención y Entrega (Euro-orden) cuya entrada en vigor en España se prevé para el primer trimestre del presente año.

En cuanto a la protección de la propiedad intelectual, a partir de ahora, no será necesario denuncia previa para la persecución y decomiso de los discos y DVD piratas vendidos por los "manteros" en las aceras de las calles, puesto que se ha modificado el artículo 282 de la Ley de Enjuiciamiento Criminal. Será posible, por otra parte, la persecución de los fabricantes ilegales y la incautación de los instrumentos necesarios para la realización de las copias. Medida que entrará en vigor el 28 de Abril de 2.004.

En general se endurecen las penas por los delitos contra la propiedad intelectual.

Se incluirán como agravantes de las penas el uso de menores en los actos delictivos, la reincidencia y la pertenencia a organización delictiva.

En cuanto a la habitualidad, la comisión de cuatro faltas se convertirá en un delito.

El nuevo Código Penal endurecerá las penas en los delitos de violencia doméstica.

Las agresiones aisladas serán consideradas delito, y no faltas, lo cual endurecerá las penas.

Será obligatorio acordar la pena de alejamiento, cuya duración pasa de 5 a 10 años. Mientras esté vigente, se suspende el régimen de visitas, comunicación y estancia con los hijos.

El maltrato a los animales estará regulado en la nueva norma, así como la violencia en el deporte.

Se modifican los artículos 89 y 108 C.P. y se sustituye la pena de privación de libertad inferior a seis años por la repatriación y la prohibición de volver a España los diez próximos años.

Se modifica el artículo 149 C.P. incluyendo como delito de lesión la mutilación genital.

## INICATIVAS EUROPEAS

### Protección de datos

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

98

- Armonizar las legislaciones nacionales relativas al tratamiento de datos personales y proteger a este respecto las libertades de las personas, en particular el derecho a la intimidad.

- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [Diario Oficial L 201 de 31 de julio de 2002].

- Proteger el derecho a la intimidad en lo que respecta al tratamiento de los datos personales en el sector de las comunicaciones electrónicas.

### Propiedad Intelectual

- Libro verde de la Comisión Europea, de 27 de julio de 1995, sobre los derechos de autor y los derechos afines en la Sociedad de la Información.

- Decisión del Consejo, de 16 de marzo de 2000, relativa a la aprobación, en nombre de la Comunidad Europea, del Tratado de la OMPI sobre derecho de autor y del Tratado de la OMPI sobre interpretación o ejecución y fonogramas.

- Directiva del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines en la sociedad de la información.



## **Comercio Electrónico**

- Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior ( Directiva sobre el comercio electrónico) [Diario Oficial L 178 de 17.07.2000].

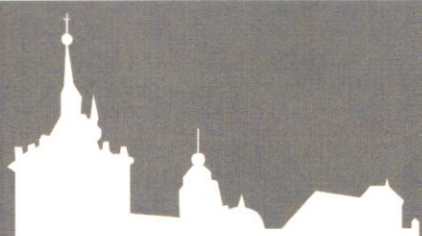
- Propuesta de Directiva del Consejo por la que se modifica la Directiva 388/77/CEE relativa al régimen de imposición sobre el valor añadido aplicable a determinados servicios prestados por vía electrónica.

- Comunicación de la Comisión de 18 de abril de 1997:Una iniciativa europea en el sector del comercio electrónico.

- Decisión nº 276/1999/CE del Parlamento Europeo y del Consejo, de 25 de enero de 1999, por la que se aprueba un plan plurianual de acción comunitaria para propiciar una mayor seguridad en la utilización de Internet mediante la lucha contra los contenidos ilícitos y nocivos en las redes mundiales.

**SEGUNDO PANEL**

**VULNERABILIDADES Y CIBERAMENAZAS**



# **DELINCUENCIA TECNOLÓGICA**

**Miguel García Izquierdo**  
**Comisario del Cuerpo Nacional de Policía.**  
**Jefe de la Unidad Central de Inteligencia Criminal**

## **PRESENTACIÓN**

Quisiera agradecer en primer lugar a la Universidad Complutense de Madrid y al Instituto de Estudios de Policía la oportunidad que me brindan para aportar una visión de los delitos que se llevan a cabo a través de la red en nuestro país, en la medida que podemos acotar esta territorialidad, pues el ámbito sin fronteras de Internet aporta una nueva dimensión en la investigación de este tipo de delitos, en función de las peculiaridades de los distintos Estados, legislación, desarrollo, tratados etc.

103

La visión que les voy a exponer es bajo el aspecto eminentemente policial, desde la Brigada que en el Cuerpo Nacional de Policía tiene la misión de la investigación policial, la BIT, (Brigada de Investigación Tecnológica) en la que estuve al frente en el pasado año.

## **EL ESPACIO VIRTUAL COMO MARCO PARA LA NUEVA DELINCUENCIA**

Creo que una breve visión de la génesis de Internet es precisa para tener una mejor perspectiva de lo que es Internet. Aquí ya nos han hablado de redes, de riesgos, de ataques, de virus, de túneles de comunicación, pero quisiera hacer una pequeña precisión de, cuándo, dónde, por qué y cómo se crearon.

Internet se inició como un nuevo sistema de comunicación hace más de 30 años por el Departamento de Defensa de los EEUU como instrumento para estrategia militar y que seguidamente en cooperación con otros centros de investigación en este caso las universidades norteamericanas, debido a la concepción que tienen los norteamericanos de la defensa,



lo cierto es que con la financiación de Defensa los investigadores informáticos contaron con los recursos precisos para sus trabajos, y el desarrollo de investigaciones aportó como resultado que los investigadores Vinton Cerf, y Bob Khan en el año 1973 crearan el protocolo TCP/IP, Transmission Control Protocol/Internet Protocol (TCP/IP). TCP convierte los mensajes en pequeños paquetes de información que viajan por la red de forma separada hasta llegar a su destino donde vuelven a reagruparse. IP maneja el direccionamiento de los envíos de datos, asegurando que los paquetes de información separados se encaminan por vías separadas a través de diversos nodulos, e incluso a través de múltiples redes con arquitecturas distintas; como aquello funcionó continuó desarrollándose dando lugar a la mayor red de comunicaciones que nadie pensó llegaría a convertirse en la impresionante fuente de negocio y de implantación en todos los sectores de la sociedad actual.

En la década de los ochenta empezamos a familiarizarnos con los ordenadores, esa máquina o computadora que por sí sola no tiene otra utilidad, que permitir poder realizar una serie de tareas acorde a unos programas establecidos, utilizarlo como máquina procesadora de textos y para ejecutar cualquier programa previamente cargado.

104

Sin embargo cuando conectamos un ordenador a una red salimos de nuestro ámbito doméstico a la red de autopistas que conectan con todas las partes del globo; nos metemos en el "ajetreado tráfico" podemos viajar, tener acceso a ingentes cantidades de información, ver, comprar, establecer contactos y también ser víctimas de los desaprensivos, pues ese terminal, máquina o PC conectado a una red, es un instrumento perfectamente válido para realizar acciones delictivas. ¿Cómo podemos hacer todo esto?. Pues sencillamente por que los ordenadores se comunican entre si, lo hacen a través de los diferentes protocolos que tienen asignados para distintas utilidades; el protocolo ideado por Vinton Cerf TCP/IP, TCP (garantiza que llega el paquete de envío de información a modo de acuse de recibo) es el que permite estas conexiones. La dirección IP, compuesta por cuatro bloques de cifras entre el 0 y el 255 y separadas por puntos es, digamos, la matrícula de un ordenador cuando se conecta a la red y le acompaña mientras dura la sesión de navegación y es la que en la investigación policial toma auténtico protagonismo para la identificación de los responsables de actos punibles.

Mencionar que como acontecimiento clave en la historia reciente de Internet, en 1992 se desarrolló el protocolo http, las tres www, World Wide Web o tela de araña mundial, en el Laboratorio Europeo de Física en Suiza. Esta tecnología provocó un drástico cambio en la apariencia, en el sentido y en el uso de internet, aumentan las posibilidades de conexión y a más velocidad, apareciendo los servicios gratuitos, se generaliza el correo electrónico y florece un nuevo mundo comercial e industrial que lógicamente inyecta dinero y donde hay dinero o vías para conseguirlo aparecen delincuentes o nuevos delincuentes.

## **TIPOLOGÍAS DELICTIVAS MÁS FRECUENTES EN EL ESPACIO VIRTUAL, CARACTERÍSTICAS DE LAS MISMAS**

### **TENDENCIAS Y DIFICULTADES QUE LA POLICÍA ENCUENTRA PARA TRABAJAR EN ESTE NUEVO ESPACIO**

Entre la tipología más frecuente en el espacio virtual, podemos considerar perseguibles de oficio la distribución de pornografía infantil a través de la red y los relativos a la infracción de los derechos de autor en los casos en que la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

Las actividades delictivas relacionadas con las nuevas tecnologías, podemos encontrarlas en forma de “nuevos delitos específicamente relacionados con la red” y las nuevas formas de comisión o nuevos “modus operandi” en delitos tradicionales ya conocidos.

En las nuevas conductas antisociales y, por ende podrán catalogarse como delictivas, consideramos las intrusiones, por englobar aquí todo aquello que de manera específica tiene que ver con la seguridad de los sistemas informáticos o “hacking”. Básicamente consistirían en la obtención de información de sistemas informáticos de terceros mediante accesos no autorizados, las prácticas de “ingeniería inversa” para la eliminación de los sistemas de seguridad en los programas de software (“cracking”) y los daños o coacciones mediante ataques de denegación de servicio a máquinas de grandes comerciales.

#### **El hacking**

Su sistema de intrusión se basa en la localización de accesos desprotegidos, los sistemas que albergan complejas y grandes aplicaciones compuestas de guiones con millones y millones de líneas de programación. No es fácil imaginar que los programadores puedan haber previsto todas las posibles situaciones del enorme conjunto de sus múltiples variables, pues algunas de esas situaciones no previstas son los llamados “agujeros o Bugs” y constituyen un peligro para la seguridad del sistema. Una vez que han tenido acceso a la red, pueden causar auténticos estragos, robar información, dañar / destruir archivos / aplicaciones.(Artc 197 del C.P).

Hacer en este apartado una consideración sobre una de las conductas más habituales del “hacking”, consistente en el escaneo de puertos y la mera entrada sin autorización en una máquina, en las que no se pueda acreditar que se ha procedido a dañar, apoderar, modificar, ni siquiera abrir esos ficheros y que por tanto podrían no ser conductas típicas en nuestro Código Penal. El escaneo o exploración de puertos, que consiste en enviar sistemáticamente paquetes de información a distintas máquinas de la red o a distintos puertos de una máquina concreta, pudiera ser contemplado como actos preparatorios para una acción posterior. Es muy habitual los



comunicados normalmente a través de correos electrónicos donde los internautas informan de haber detectado escaneos o accesos sin más. Como ejemplo digamos que sería una conducta similar a aquel individuo que caminando por una calle va comprobando las cerraduras de los vehículos al lado de la misma conducta que no puede ser considerada como punible, aunque si le convertiría en un hipotético sospechoso ante la comisión de un hurto en el interior de vehículo en dicha zona en un entorno temporal coincidente. Normalmente estos sujetos, raramente persiguen una máquina o usuario en concreto de la misma manera que nuestro delincuente virtual de vehículos no busca uno determinado, sino aquel que presente fallos de seguridad —que no haya cerrado la puerta—, estas son las conductas más habituales del “hacking blanco o recreativo” que a priori no persiguen descubrir secretos o vulnerar la intimidad de nadie salvo que una vez cometido el acceso a la máquina, se acceda también a la información. Para otros hackers, su hooby es, tras el acceso, dejar su aviso unas veces al usuario de esa vulnerabilidad u otras veces, como hizo hace poco tiempo un hacker mexicano sobre fallos en una aplicación de Microsoft, lo dio a conocer pero a través de la red.

Otros, una vez han accedido, se les despiertan otras intenciones, como es el caso de un joven detenido a finales del pasado año que tras acceder a una máquina y comprobar que albergaba ficheros con documentos de interés, establece contacto con aquel usuario advirtiéndole que “había observado como le robaba ficheros un hacker pero el había conseguido recuperar alguno de estos”, facilitándole teléfono de contacto para la devolución, cita a la que asistimos, donde devolvió los ficheros, “a la vez que expuso sus tarifas por ofrecer un servicio integral de seguridad informática”.

106

## Crackers

Tiene varios significados este término, uno de ellos el que le otorgan los “hackers” que de alguna manera hemos descrito anteriormente, serían los “hackers no éticos”, que una vez que han tenido acceso provocarían daños en la máquina. Pero el mayor interés de este término se suscita como desarrollador de “ingeniería inversa” procedimientos por los que se logra burlar los sistemas de seguridad de los paquetes de software.

La trascendencia de esta actividad soporta unos costes económicos elevadísimos, ya que en buena medida son responsables de una gran parte de las acciones de “pirateo” de software y cómo no del DVD o “DivX” (desprotección del DVD e interpretación para lectura con lector de CD de un ordenador) es decir de la industria cinematográfica.

## Insiders

Este grupo que correspondería a empleados desleales o descontentos o antiguos empleados y conocedores de los sistemas de seguridad informáticos de la empresa así como de cuentas / contraseñas de acceso que



suelen seguir estando operativas tras sus cambios de destino o despidos, son unos de los que más incidencias reportan. Por este tipo de autores son habituales las llamadas “bombas lógicas”, consistentes en unas secuencias de código dañino que introducidas en una máquina, esperan a que se den unas determinadas condiciones prescritas por su programador, normalmente un perfecto conocedor del sistema y muy difíciles de detectar. Encuesta realizada entre empresas hace un año, representan entre el 57 a 70% de las incidencias.

### **Ataques de denegación de servicio**

Estos ataques por peticiones de servicio son los más dañinos y difíciles de evitar. Consisten en colapsar los servidores por inundación del tráfico, sobrecarga del número de conexiones que habitualmente se hacen falsando el origen y como Internet fue diseñado para comunicar y dar siempre respuesta al servidor atacado, prepara los recursos para dar respuesta que nunca se satisfacen por no existir el peticionario o no estar en situación de recibir lo pedido. Estas peticiones desde distintos lugares colapsa, las conexiones dejando sin servicio a millones de clientes y generando pérdidas cuantiosas.

“Mafiaboy”, es el apodo o nick de un chico canadiense de 15 años, que mediante ataques de denegación de servicio, causó daños a los servidores de famosas empresas como Yahoo, eBay etc por valor de 1700 millones de \$ según la acusación.

107

Existen múltiples variedades de bloquear servidores mediante peticiones o envío masivo de información, introduciendo previamente un troyano en los ordenadores de otros usuarios, que harían la función de “zombies” cuando “el master o director” les ordene actuar enviando peticiones de servicio o cualquier otra función, pero ni siquiera es preciso poseer estos conocimientos, uno de los métodos más antiguos es el “mail bombing”, que consiste en suscribir a la víctima a “grupos de noticias”, a unas decenas o centenares de grupos de noticias, que a su vez le remitirán centenares de noticias diarias cada uno de ellos, colapsando el ancho de banda de la víctima y tirando su sistema, entre otros.

## **NUEVOS PROCEDIMIENTOS EN DELITOS TRADICIONALES**

Las Nuevas Tecnologías de la Sociedad de la Información, pueden servir y de hecho así ocurre, para ser instrumento del delito en cualquier modalidad criminal. Los nuevos “modus operandi”, creados por los delincuentes más ingeniosos y estudiosos de asegurar sus resultados de la manera más eficaz, que más dificultades presenten a los investigadores, y si es posible que abarquen en una sola o en cómodas acciones a un mayor número de víctimas. Para ello Internet se presta como un terreno fértil, por

su rapidez, amplia difusión, sensación de anonimato e impunidad, compleja territorialidad para su persecución y enjuiciamiento.

La mayoría de la tipología tradicional, se dice, es susceptible de ser cometida a través de Internet: delitos contra las personas, robos con fuerza anulando los sistemas electrónicos de seguridad de un recinto, estafas, contra la libertad sexual, suplantación de personas, amenazas, coacciones, extorsiones. etc. Cualquier acto susceptible de control por medios informáticos y conectado a una red.

Los delitos más habituales suelen ser los siguientes: injurias, calumnias y amenazas

La mayoría no suponen delitos graves, pero la sensación de anonimato y por tanto impunidad que aporta la suscripción de cuentas de correo gratuitas sin comprobación alguna de la identidad real, o el uso de espacios como tableros electrónicos o "boards" igualmente anónimos y gratuitos encuentran un Internet un espacio muy atractivo. El envío de mensajes anónimos amenazantes incluyendo detalles personales de la víctima causan un fuerte impacto en quien los recibe, siendo uno de los hechos más denunciados, al igual que los anuncios generalmente con ofrecimiento de servicios sexuales a los que se añade dirección o teléfono de la víctima e incluso su fotografía y que finalmente suelen sustanciarse como faltas por vejación leve.

108

## DISTRIBUCIÓN DE PORNOGRAFIA INFANTIL

Entendemos por material pornográfico infantil "el material pornográfico en cuya elaboración hayan sido utilizados menores de edad."

No se especifica lo que delimita el concepto pornográfico. En la mayor parte de los países europeos y la normativa estadounidense, describen lo que se entiende por material pornográfico u obsceno, excluyendo de este concepto el mero desnudo.

Una ventaja de la ley española puede radicar en que permite al juzgador decidir la naturaleza pornográfica o no de unas imágenes dadas en razón de muchas variables de su contexto.

La casuística que queda fuera del artículo 189, b es:

- La mera tenencia de material pornográfico infantil. No penada en España y Portugal .
- La "pornografía virtual de menores", en cuya elaboración no han sido utilizado menores de edad.
- La provocación: incluyendo conductas como la demanda en los foros de Internet de este tipo de material, o la publicación de



relatos que describen prácticas sexuales o sádicas de menores y adultos, o menores y animales.

Cabe preguntarse, si unos relatos de esta guisa, deben quedar amparados por el derecho constitucional a la Libertad de Expresión.

También es este el momento de mencionar, siquiera de pasada, el problema que representa la pornografía virtual (Hentai, dibujos animados de carácter pornográfico, que puede ser dirigida a niños o digitalización de imágenes) en la que diseños hiperrealistas consiguen efectos muy próximos a la fotografía pero en los que, no obstante, ningún menor es utilizado. Parece claro que en la letra de la ley el bien jurídico protegido es el menor concreto y no algún ente abstracto como "la infancia".

En otros países europeos se hace referencia a imágenes en la que aparezcan representados menores de edad, incluidos los dibujos, y también se contemplan como típicos los relatos conteniendo descripciones de sexo con menores.

En cualquier caso son consideraciones "menores", atendiendo al material de pornografía infantil que se presenta actualmente en la red, las imágenes que estos sujetos intercambian y difunden no consiste solamente de fotografías de menores desnudos o en situaciones obscenas, se trata de actos sexuales aberrantes con lactantes y bebés de escasos meses de edad.

109

### **CONSIDERACIONES SOBRE LA PORNOGRAFÍA INFANTIL EN INTERNET**

La paidofilia y la pederastia no son nada nuevo, desde luego el surgimiento y desarrollo de Internet les otorga una dimensión y naturaleza nueva.

Son varias las características que Internet que la hacen un medio idóneo para las personas con intereses sexuales en menores de edad: la aparición de los sistemas de imagen digital, video, que puede tratar sin acudir a laboratorios comerciales y por tanto, de manera anónima, así como la transmisión de ficheros (formatos gráficos y de vídeo) de un rincón a otro del globo por un coste nimio; en segundo lugar, estas transacciones pueden realizarse desde posturas e identidades anónimas o ficticias.

En definitiva, de un paidófilo que ha de arriesgarse a ser sorprendido mientras toma fotografías de niños, o que debe mostrar su rostro o aportar datos de identidad para adquirir o intercambiar material pornográfico, pasamos a uno que desde la intimidad de su habitación accede a un sinfín de recursos gráficos sin peligro aparente de que su identidad y personalidad pueda ser descubierta.

Pero si estos elementos son preocupantes de cara al impacto que puedan suponer en cuanto a disponibilidad de material pornográfico infan-



til en la Red, no lo son menos las posibilidades que la Red otorga a la constitución de una Comunidad Paidófila, donde al miembro de una comunidad "le identifica, le refuerza y le asiste en su conducta desviada", proporcionándole no sólo el material gráfico para aliviar sus necesidades, o la información necesaria para satisfacerlas plenamente, sino una razón de ser, incluso albergando la posibilidad de que la pederastia sea en el futuro una legítima opción sexual más.

La pornografía infantil es un hecho penalmente reprobable en la mayoría de la legislación mundial, por cuanto promueve la agresión a menores, en la necesidad de incorporar nuevo material ya que las imágenes digamos "caducan" con el uso o pasan a formar parte de colecciones que nunca se consideran completas.

No obstante, gracias a Internet y a la acción policial se puede identificar a individuos pederastas, potencialmente peligrosos, que tal vez en otro caso nunca hubieran sido descubiertos, sino tras la comisión de un acto de tintes dramáticos. No olvidemos que la lucha contra pornografía infantil no es otra cosa que un tratamiento sintomático de otro fenómeno mucho más grave, la agresión sexual y abuso a menores de edad. Recientemente se ha detenido en Perú a un matrimonio pedófilo por investigaciones iniciadas en España que llegaron a Perú a través de INTERPOL por elaboración de vídeos realizando agresiones sexuales a una niña de cinco años.

110

## FRAUDES A TRAVES DE LA RED

El comercio encontró en Internet un medio ágil de penetración y de expansión y como no podía ser de otra manera donde aflora el dinero, aparecen sujetos dispuestos a apoderarse de lo ajeno. La tipología penal tradicional y algunas nuevas formas de comisión "modus operandi" encuentran por las características de Internet un lugar ideal para estas actividades criminales.

La casuística más extendida es la relativa a la comisión de fraudes mediante los datos de las tarjetas de crédito para la compra en comercios virtuales.

Las tarjetas fueron concebidas para su utilización material, lo que no es posible a través de Internet. En un principio para el comercio virtual y en muchos aún hoy día era suficiente con que el número de la tarjeta estuviera bien construido, respetando unos determinados códigos asignados a cada entidad bancaria y el resto que cumpla una condición matemática más o menos sencilla. Con esto, no tardaron en aparecer programas generadores de números válidos de tarjetas (conociéndose los códigos de las entidades bancarias y algoritmos de formación de números), con los que era posible realizar compras en este tipo de comercios. Posteriormente se añadió como seguridad adicional la fecha de caducidad que sigue siendo una medida débil. Independientemente de la construcción de números de tar-

jetas válidos, el conocer los datos contenidos en la cara estampada de la tarjeta es suficiente para poder realizar compras a través de Internet.

Estos datos son susceptibles de obtenerse de muchos modos, se dice que los hackers establecen “sniffers” en las redes por las que circula la información para obtenerla y hacer uso de la misma. Para evitar este riesgo se han desarrollado conexiones seguras (SSL) y tecnología VPN (conexión remota segura en un túnel encriptado entre empresas o usuarios remotos). No obstante bastante más riesgo de que se apoderen de nuestros datos en Internet tenemos en la vida real; es habitual que al hacer pagos con la misma la perdamos de vista durante algún tiempo, con el riesgo de que empleados desleales de restaurantes o comercios las obtengan. Números que pueden ser objeto de intercambio entre sujetos de distintos países en canales de IRC, complicando sobremanera las acciones policiales de unos y otros.

## SUBASTAS EN INTERNET Y VENTAS FICTÍCIAS

Existen sitios web que proporcionan al usuario de Internet la posibilidad de vender, intercambiar, adquirir mercancías o subastas.

Estafadores acuden a estas páginas ofertando productos, generalmente informáticos a precios muy favorables a los que se pone un precio de salida o venta directamente por el que los usuarios se interesan. El dinero se envía y el producto nunca llega.

111

En el anuncio suele facilitarse un número de teléfono móvil incluso una cuenta de correo electrónico, facilitándose para el envío del dinero una cuenta bancaria. Se está generalizando el pago a través de intermediarios o servicios o empresas de “escrow”; estas actúan a cambio de un pequeño porcentaje o comisión entre vendedor y comprador, ambos remiten producto y dinero y con la conformidad por parte de este servicio de una transacción correcta reenvía a cada uno mercancía y dinero. El pasado año se efectuó la detención de cuatro personas que tras remitir a su víctima a un servicio de estas características, para cerrar la operación y ver las garantías que se ofrecían, le señalan que para mayor efectividad se dirija al delegado en España de aquella firma, que se haría cargo del dinero, que no era otro que un miembro más del grupo de estafadores.

## SOLICITUD ENGAÑOSA DE TARJETAS

Se realiza mediante la apertura de cuentas en banca on-line utilizando documentación personal falsa y buzones preparados para recoger la información bancaria. Se solicitan tarjetas de crédito para lo que se aportan nóminas falsas, datos laborales, que permitan cuantías elevadas en las disposiciones con las tarjetas. Luego quedan en descubierto. El pasado año en una localidad catalana se desarticuló un grupo que incluso disponían



con la infraestructura de una gestoría de uno de los detenidos para la obtención de datos laborales y nóminas falsas.

## **CARTAS NIGERIANAS**

Este procedimiento así denominado por ser la mayoría de sus autores de esta nacionalidad, o hacen referencia a operaciones en aquel país viene a ser una variante de nuestros tradicionales timos de la “estampita” o el “toco mocho” tecnológicos. Se envían a través de correos electrónicos (las direcciones pueden obtenerse simplemente en los listines públicos o en múltiples foros de la propia web) a ciudadanos de países como Arabia Saudí, Jordania, Nueva Zelanda, etc, en las que anuncian que han sido agraciados con un premio del Gordo de la Primitiva sobre una serie de boletos que aleatoriamente se asignan a ciudadanos de diversos países. Facilitan teléfonos de contacto y al que llama le envían toda una carpeta de documentación con sellos de todo tipo, premio, compañía aseguradora que tiene el premio en su poder y plazo para la retirada, debiendo satisfacer el importe de los impuestos para su retirada o de lo contrario el premio será ingresado en las arcas de Hacienda. Tras llamadas con los supuestos responsables de compañías aseguradoras, bancos etc, el pago suele realizarse a través de transferencias a cuentas abiertas con documentación falsa o empleando circuitos de banca on-line de más de un país o a través de entidades multinacionales de pago o envío de dinero.

112

Otras modalidades aluden a participar en transferencias de fondos gubernamentales, excedentes de presupuestos para lo que exigen unas cantidades para pagar comisiones, sobornos etc.

## **SOLICITUD ENGAÑOSA DE TRANSFERENCIAS**

Es el envío masivo a empresas ofertándoles la posibilidad de ser incluidas en un registro o listín de Internet para lo cual tienen que remitir una cantidad de dinero a la cuenta bancaria que se les indica.

## **COMERCIOS VIRTUALES**

Comercios virtuales que se abren sin el debido control de legalidad de algunas entidades bancarias que les dan el servicio de pasarela y donde posteriormente son utilizadas tarjetas de manera fraudulenta simulando compras y retirando el efectivo en los días que se tarda en detectar el fraude de cargo en las tarjetas

## **PIRATERIA**

### **Propiedad Intelectual**

Entre los delitos que pueden llamarse “informáticos” se encuentran dos radicalmente distintos en cuanto al reproche social que suscitan: de una



parte está la distribución de pornografía infantil por Internet, con una pena máxima de tres años, y enérgicamente rechazada por la ciudadanía; de otra están los delitos relativos a infracciones de los derechos de autor, con penas semejantes, de hasta dos años, que no suscitan, en general, el menor reproche.

### **Modus operandi**

Antes de hablar de ilícitos penales en esta materia, permítanme introducir el concepto de “warez”, que proviene de “wares”, del inglés, “mercancías”, que podría traducirse como “mercancías informáticas pirateadas”, es decir, en general “programas pirateados” o programas en los que de forma no autorizada se ha suprimido o neutralizado el dispositivo técnico utilizado para protegerlo.

Basta con introducir este término “warez” en un buscador para darse cuenta de lo extendida que está esta práctica<sup>(1)</sup>. De modo complementario, otra forma de procurarse un uso gratuito de las aplicaciones informáticas consiste en proveerse de las llamadas versiones “trial” o “demo”. Estas versiones de prueba o evaluación tienen limitado su uso a un periodo de tiempo determinado, o no son completamente funcionales. Su razón de ser no es otro que el posible comprador tenga una muestra bastante para decidirse o no por su compra. En la mayoría de los casos es exactamente esa versión trial o demo la que va a ser completamente funcional y sin limitación de tiempo una vez haya sido adquirida la licencia y el vendedor haga llegar al comprador los códigos para eliminar las limitaciones ... o una vez se obtenga por otros medios, por ejemplo a través de alguna web de Internet. Lo que va a encontrarse en Internet para conseguir la supresión no autorizada o la neutralización del dispositivo técnico que se haya utilizado para proteger el programa de ordenador es un pequeño programa denominado “crack”, un número de serie, o un “keygen”, generador de códigos válidos.

113

### **El artículo 270 e Internet**

Del mismo modo que la aparición del disco compacto y las regrabadoras cambiaron por completo el panorama de la distribución no autorizada de programas de ordenador y música, la banda ancha y las aplicaciones “peer to peer” han terminado de globalizar y generalizar este fenómeno.

La venta de estos discos por correo postal, mensajería después de publicitar el producto por Internet, parece que no ofrece duda en cuanto a su tipicidad, por cuanto es inequívoco el ánimo de lucro y el perjuicio de terceros.

1.- A fecha de 3.7.3, en el buscador [www.google.com](http://www.google.com) aparecen 17.800.000 páginas que contienen este término

Los hechos consistentes en transferencias de material “warez” a través de Internet, sin embargo, son más resistentes a estos argumentos. Las tarifas planas y los anchos de banda propios de ADSL o cable han permitido que puedan obtenerse cantidades de software, música, o cine sin licencia, semejantes a las que caben en un CD, en una sola noche de descarga; aunque con una notable diferencia, sin que se requiera ninguna contraprestación económica.

En tales circunstancias también aparecen serias dificultades para apreciar ánimo de lucro, sobre todo en transferencias peer to peer en las que, si existe publicidad, no la explota quien distribuye este material warez.

La gran mayoría de las actuaciones policiales por infracción de los derechos de autor se originan en la denuncia de los representantes legales de los titulares de estos derechos.

¿Cómo investigamos todas estas nuevas actividades delictivas y qué dificultades encontramos?

114

La BIT en la Comisaría General de Policía Judicial, con una estructura de dos secciones operativas y una técnica, tiene sus orígenes en el Grupo de Delitos Informáticos creado en 1975 y con cuatro funcionarios en sus comienzos. No olvidemos que según datos estadísticos en 1996 contábamos con una población internauta de poco más de 200.000 usuarios. Luego, desde el Cuerpo Nacional de Policía fue casi inmediata la concienciación de contar con los recursos humanos y materiales para dar respuesta a nuevas formas delictivas emergentes.

Una gran dificultad en conocer la situación real delincidencial es que Internet conlleva una importante cifra negra de delitos, delitos de intrusiones que no se denuncian, el usuario piensa que las acciones de los “malos” pueden consistir en enviarte un virus y para esto están los antivirus y en caso grave se formatea el disco duro, a pesar de perder toda la información que se poseyera, asumiendo esta circunstancia como algo implícito en la red. Creo ello es debido a que no existe sensación de inseguridad en la red. A nivel de empresas corporaciones, los responsables de seguridad, seguridad lógica, rara vez comunican una incidencia tal vez, por evitar la sensación de inseguridad o vulnerabilidades a la firma.

Bien es cierto que existe, como en todo el aspecto positivo, que es extraordinaria la colaboración de los internautas en general, que comunican mediante correos a las cuentas de la Policía, incluso de otros países y esencialmente cuando se refieren a contenidos en castellano, a algún ISP español o ingentes cantidades de información sobre aquello que les despierta sospechas o consideran delictivo, las respuestas de agradecimiento, acuse de recibo o solicitud de contacto, hace que para algunos se intensifiquen los rastreos en busca de contenidos ilícitos en la red, para reportarlo a la Policía, al igual que ocurre el área de pornografía infantil donde las ONG,s españolas se muestran en un alto grado de colaboración informando igualmente de estos contenidos.



## DIFICULTADES

El modelo de distribución e intercambio de pornografía infantil basado en servidores de ficheros con banda ancha, concurriendo los usuarios con clave de acceso desde un canal secreto de IRC, parece ser uno de los modelos que cabe esperar en el futuro. Junto con el anterior, parece que se imponen con fuerza las aplicaciones “peer to peer” tipo KazaA, Morpheus, Edonkey, Audiogalaxy, Bear y otros, cuyas principales problemas para la investigación radican en la dificultad de discriminar la conexión TCP que transmite un determinado fichero, o él que el mismo se transmita fragmentado desde varios orígenes o el que un determinado usuario pueda descargar un fichero ilegal en su máquina y después transmitirlo a un tercero sin su conciencia ni voluntad.

No disponemos de demasiados elementos para la investigación en Internet. El indicio más básico es la dirección o número IP de origen que creo Vinton Cerf, es el número que nos identificará la máquina conectada a una red, y que va embutido el propio protocolo TCP/IP. La misión de este protocolo es asegurar la transmisión de modo que los posibles paquetes se reenvíen en caso de pérdida o llegada defectuosa, y para ello se necesita la colaboración de la máquina receptora, que en gran número de casos corresponde a la víctima. Como en cualquier investigación policial procuramos situarnos en el lugar del crimen y hacer el camino inverso rastreando todas huellas, hasta el momento que provistos del mandamiento judicial podamos llamar a la puerta de nuestro presunto autor.

115

El protocolo IP establece un sistema de direcciones que identifica de forma clara y precisa la máquina emisora y receptora de un paquete de datos. A través de este número conocemos la red a la que pertenece la máquina en primer lugar y a la máquina concreta dentro de esa red en segundo. Una vez obtenida esta dirección del examen del documento que da lugar a la denuncia o del que en general inicia la investigación pasamos a realizar las gestiones para determinar quién fue el usuario de esa máquina en el momento en que tuvieron lugar los hechos precisando de mandamiento judicial para la práctica de esta diligencia.

El titular de esa dirección IP, normalmente un ISP, o una institución privada o pública, deberá informar de una determinada consola o cliente junto con el número de teléfono desde el cual se realizó la conexión. En adelante y tras esta primera fase de investigación específica sobre la red, se llevan a cabo las indagaciones o diligencias de manera tradicional que puedan proceder, toma de declaraciones, vigilancias, entradas y registros etc. En esa primera fase de “investigación virtual” creemos es de carácter indiciario, entendiendo que el resultado del resto de la investigación, digamos “investigación tradicional” como registro del ordenador, aportes de documentación bancaria en caso de operaciones con ánimo de lucro etc, son las que realmente aportarán elementos de juicio.



## Territorialidad

La investigación en Internet, tiene una problemática añadida que afecta a todas las policías del mundo. El espacio de Internet carece de fronteras, y frente al posible envío de un paquete de datos de contenidos ilícitos como pornografía infantil que en milisegundos circula de un país a otro, la investigación en muchas ocasiones desemboca en la petición de Comisiones Rogatorias que se nos demoran en el tiempo perjudicando gravemente el resultado satisfactorio de la investigación y siempre que los hechos que se persigan en un país igualmente estén tipificados en aquel al que supuestamente deba solicitarse la información. Recordemos que en el año 2000 el famoso virus I Love You causó daños al infectar a más de 60 millones de ordenadores en todo el mundo, siendo el responsable un estudiante de informática de Filipinas, acción que fue el primer ciberdelito en aquel país sin legislación que recogiera tal acción y según mi información quedó impune al no estar la acción tipificada en la legislación Filipina.

Mencionamos antes que los delitos contra el honor ocupan un volumen importante de las denuncias recibidas. La investigación de estos hechos, que como se comento suelen ser tipificados de faltas, en muchos casos pasan por la expedición de tres Mandamientos Judiciales:

116

- Al responsable del tablón o foro electrónico, cuando la difusión se hace por este medio ya que muchos tabloneros no incorporan la información correspondiente a la IP de origen.

- Al Proveedor de servicios que informaría del usuario de esa IP en el momento de la publicación del mensaje, en cuya respuesta como dato de valor sería la que señale la línea telefónica desde la que se realizó la conexión, que no tiene por qué coincidir con el titular de la cuenta de acceso a Internet, y si el número es de los declarados secretos.

- Mandamiento dirigido al operador telefónico. Para un exacto cumplimiento en la obtención de todas las pruebas, sería lógico proceder a la intervención y estudio del ordenador emisor, en cuyo caso por un hecho tipificado como falta difícilmente se justificaría una entrada y registro en un domicilio.

La investigación de los delitos que tienen lugar en la red o desde la red requiere la retención de los datos del tráfico por parte de los proveedores de servicio, pues será lo que informe un determinado proveedor sobre el usuario concreto que ha estado usando una dirección IP, lo en buena medida que determine el curso de la investigación.

La LSSI-CE en su artículo 12 establece el plazo máximo que los proveedores de servicios podrán retener estos datos, que lo fija en 12 meses y deja para el futuro reglamento qué datos de tráfico deben registrarse y retenerse, y por cuanto tiempo. Es esta una herramienta legal imprescindible para la investigación de estos delitos y al menos asegurar a las víctimas

tener cauces de investigación, que no olvidemos, siempre son solicitados por la Policía con ocasión de un hecho delictivo cometido y en un proceso judicializado.

## CÓMO PODEMOS MEJORAR LA RESPUESTA

Creo que Internet es uno de los terrenos más agradecidos para la prevención en materia de seguridad, en base a la concienciación de los usuarios, no prevención en los términos policiales propiamente dicha, que sería impensable con cientos de millones de ordenadores conectados simultáneamente y millones de páginas que puede indexarnos cualquier buscador.

En un alto porcentaje, (sobre todo y son mayoría los internautas más jóvenes) se usa Internet “como si fuera un juego mas de ordenador”. Salir a la red aconseja conocer unas reglas de utilización tanto para los más jóvenes como para adultos dentro del ámbito de usuario doméstico o privado, tanto en contactos con personas desconocidas, en el uso del correo electrónico, en la propia seguridad de nuestro equipo, en la información que nosotros podemos facilitar personal a través de la red, y en operaciones de carácter económico. Ahora entidades de tarjetas de crédito han implantado el CES, que permite hacer compras seguras en la red. Las tarjetas previamente se registran en el programa CES que autentifica mediante una clave adicional y los comercios adheridos al sistema sólo admiten el pago con tarjetas previamente registradas.

117

Considero vital el “control” en “primer nivel” referido al ámbito familiar y escolar, de un control de los lugares que se visitan no bajo una visión represiva, pero si de estar pendientes de las compañías y zonas de recreo. Internet tiene también sus “puntos negros” y a la antigua usanza permítanme la expresión “barrios chinos” no demasiado formativos para un navegante de, tal vez, 12 años. Seremos los padres y educadores en los centros los responsables de formar adecuadamente a la futura generación y disfruten plenamente de este extraordinario instrumento que es Internet como medio de comunicación e información. Para ello existen filtros, por los ISP, e instrumentos, incluso en la propia red que nos ayudarán a una navegación más segura.

Para ello, son muy importantes las campañas de divulgación y concienciación. En las empresas, políticas de seguridad, tanto en implantación de sistemas, mantenimiento, actualización y control sobre accesos a aplicaciones o sistemas de usuarios autorizados, contraseñas seguras y custodia, gestión de la red por responsable cualificado, son medidas esenciales para evitar un altísimo porcentaje de incidencias en la red.

Regulación de los cibercafés, casi el 20% de las conexiones se realizan desde estos establecimientos, resulta curioso que debamos entregar nuestro DNI para acceder a un hotel donde sólo pretendemos descansar o para acceder a un bingo y no para acceder a una máquina desde la que podemos delinquir, enviando pornografía infantil, amenazar o estafar a alguien.



Indudablemente la redacción del Reglamento de la LSSI-CE en cuanto a la retención de datos será básico para las investigaciones y los elementos probatorios que la Policía pueda poner en manos de las autoridades Judiciales en la persecución de los delitos a través de la red. En la batalla en defensa de las argumentaciones sobre el anonimato total, y la seguridad en la red, no creo que estemos en situación de afrontar el riesgo de hacer de Internet un lugar sin capacidad para investigar y sin derecho alguno para las víctimas convirtiéndolo en un instrumento de impunidad al servicio de los delincuentes. No debemos confundir capacidad de represión de un delito con censura. Las acciones a reprimir están meridianamente claras y recogidas en las legislaciones de los países.

La formación actualizada y permanente sobre las nuevas tecnologías como campo e instrumentos utilizados para la actividad criminal dirigidos a Jueces, Fiscales y funcionarios de Policía es, con seguridad, una de las mejores estrategias y herramientas que nos podemos dar para un futuro próximo.

Es necesario potenciar la colaboración en foros internacionales y grupos de trabajo especializados (Europol, Interpol), sobre estas nuevas formas de delincuencia que se sirven de un medio como es la red carente de fronteras, que parecen haber quedado en pie únicamente para la labor de investigación policial y judicial.



## **CIBERTERRORISMO: UNA APROXIMACIÓN AL PROBLEMA**

**JUAN HIDALGO CUESTA**  
**Comisario del Cuerpo Nacional de Policía**  
**Vocal Asesor del Secretario de Estado de Seguridad**

Nunca antes en la historia de la humanidad la irrupción de nuevos inventos o nuevas tecnologías había influido tanto en la vida ordinaria de las personas ni tan rápidamente. Quizás la invención del cobre o después del hierro supusieron cambios drásticos, o quizás la invención del estribo para montar a caballo supuso una revolución considerable en su tiempo, pero todo ello tuvo lugar con un desarrollo muy lento, a lo largo de muchos años, nada parecido a lo que hoy ocurre.

Hace sólo 150 años la velocidad de la información era la velocidad de un caballo, no podía llegar más rápido a otras partes, hoy esa velocidad se ha multiplicado por millones.

Hace 100 años nuestra capacidad de almacenamiento de información se limitaba al papel. Hoy día nuestra capacidad de almacenamiento casi no conoce límites, almacenamos en muchos formatos, grabamos todo lo que pasa, todo lo que se dice, todo lo que se escribe y todo lo que se habla. La información la tenemos almacenada y rigurosamente catalogada, para que seamos capaces de encontrar lo que buscamos fácilmente, con posibilidad de interrelacionar elementos casi imposible de relacionar con el uso del cerebro humano. Además podemos acceder a esa información en tiempo real desde cualquier lugar, en cualquier momento, es decir hemos fundido nuestra capacidad de mover la información con la de almacenar y clasificar, pero el elemento definitivo ha sido el hacer que esa información sea accesible a todo el mundo, la revolución informática ha tenido mucho que ver con esto. Todo ello en conjunto ha supuesto una revolución que afecta definitivamente a nuestra forma de vivir, a nuestra calidad de vida, a todo en todos los sentidos.

No hay tiempo para trazar aquí una breve historia de la informática, ni de las telecomunicaciones, ni siquiera de la telemática, pero es obligado prestar al menos un pequeño reconocimiento a aquellos que con su visión han hecho posible todo lo que acabamos de relatar, desde los visionarios como Alvin Tofler y Arthur C. Clark, a los creadores de protocolos como Vinton Cerf y Bob Kahn.

En 1945 Arthur C. Clark, el renombrado autor de "2001: una odisea en el espacio" escribió en una revista llamada "Wireless World" un artículo en el que claramente describía una red de satélites que giraban en órbita alrededor de la Tierra. A través de estos satélites que él denominó "enlaces extraterrestres" se producían comunicaciones de alcance mundial. Tuvieron que pasar muchos años antes de que la Unión Soviética pusiera en órbita el primer satélite. Vinton Cerf y Bob Kahn coincidieron trabajando en DARPA (Defense Advance Research Project Agency) una agencia muy especial creada por Eisenhower en 1958 como respuesta al lanzamiento soviético al espacio del primer Sputnik. El temor de que ante un ataque nuclear soviético las unidades defensivas norteamericanas no pudieran comunicarse y por tanto coordinarse fue el motivo de que a DARPA se le impusiera como misión la creación de una red de comunicaciones que impidiera este supuesto. En mayo de 1974 publicaron su trabajo sobre la creación del protocolo de comunicaciones entre ordenadores que hoy conocemos como TCP/IP.

120

Hace ya muchos años que el sociólogo Alvin Tofler predijo en sus obras una red mundial que permitiría entre otras muchas cosas el "teletrabajo", describió perfectamente cómo nuestras vidas se verían afectadas por esta nueva forma de comunicación y le sirvió para describir lo que él llamó "la tercera ola", la ola que movería a la humanidad en un nuevo avance, la "ola" de las comunicaciones.

Gracias a ellos y a otros muchos que vinieron detrás, que trabajaron con sus ideas y desarrollaron los esbozos y visiones de los demás hoy tenemos la capacidad de comunicación y de compartir información que hemos descrito. Hay sin embargo un elemento común que se iba desarrollando rápidamente y que permitía todo esto: el ordenador.

Se considera que fue en 1946 cuando apareció el primer ordenador equivalente a lo que hoy conocemos como tal. Tenía esta máquina una capacidad de cálculo de 5.000 operaciones por minuto y ocupaba 90 metros cuadrados. Desde entonces su capacidad de cálculo se ha ido multiplicando por dos cada dieciocho meses y su tamaño se ha reducido a proporciones ínfimas.

Esta máquina comenzó a estar disponible para el público ordinario a finales de los años 70 y ahí comenzó la tremenda revolución. Despertó y



sigue despertando una curiosidad inimaginable, una pasión a veces incomprensible. No se le trata como a una simple máquina que hay que programar, se le trata como a una mascota, como a algo muy personal. Hay amantes y detractores de sistemas operativos, de programas, de tarjetas de vídeo. Se establecen discusiones que generan incluso odios personales sobre si una máquina es mejor o peor que otra. No se trata pues de una máquina ordinaria, es algo especial. Entendiendo este carácter especial podemos comprender el profundo conocimiento que de la misma llegan a tener personas sin formación académica desde la más tierna juventud, y también nos facilita comprender el peligro que ello acarrea.

Cuando hablamos de ordenador no nos referimos exclusivamente al más conocido, a ese que lleva monitor, teclado y ratón. Un ordenador es mucho más sencillo y también mucho más complicado de definir, un ordenador puede ser lo que conocemos como un simple chip, algo que encontramos de forma casi omnipresente a nuestro alrededor.

Ahora, casi sin darnos cuenta, dependemos de los ordenadores, forman parte de nuestra vida diaria, son una necesidad, cumplen una función que la mayoría de las veces nos pasa desapercibida porque se han integrado de tal manera en nuestra cosas que resulta difícil singularizarlos. Es posible que nos despertemos cada mañana con un despertador que lleva un chip embutido que contiene los datos necesarios para su programación diaria, semanal, etc. Muy pronto ese despertador antes de hacer sonar la alarma conectará a Internet, comprobará el estado del tráfico y decidirá a la hora que debemos levantarnos según se encuentren las carreteras. Llevamos en nuestro bolsillo un teléfono móvil que además sirve de agenda. Miramos el reloj de pulsera que contiene una base de datos de teléfonos, o mide la altura a que nos encontramos, o la velocidad a que nos movemos, o nuestras pulsaciones. Conducimos un vehículo en el que los chips se encuentran por doquier, controlan desde el sistema de inyección, a los indicadores de dirección, y es posible que hasta disponga de un GPS que nos muestre nuestra posición en un mapa de la ciudad.

En nuestro trabajo utilizamos un ordenador convencional, disponemos de otro portátil para los desplazamientos y hasta uno que cabe en la palma de la mano en algunos casos, pero incluso si no disponemos de este tipo de ordenadores, seguro que en toda oficina hay un fax que tiene el correspondiente chip embutido. En nuestras casas los ordenadores están en nuestra lavadora, en la secadora, en el horno microondas, en el VCR, en el DVD.

En muy poco tiempo estos chips serán accesibles a distancia también, integrado en nuestro frigorífico detectará las carencias y formulará pedidos a través de Internet cuando los necesite. Nuestros hijos se entretienen con ordenadores desde que son muy pequeños, desde los propios ordenadores con teclado a las consolas de videojuegos, etc, etc.



Si toda nuestra vida depende cada vez más de los ordenadores que encontramos a nuestro alrededor ¿qué podemos decir de las empresas que nos proveen de los servicios esenciales que nuestra sociedad necesita? El ordenador se ha incrustado tanto en ellos que hoy en día es imposible pensar en la prestación de esos servicios sin la ayuda de esos ordenadores, y esos servicios son tan esenciales que forman parte de la estructura de defensa del propio país.

Durante la última parte del siglo pasado el papel que la iniciativa privada en la prestación de servicios creció en todo el mundo de manera considerable, hasta el punto de que la defensa de un país puede depender en gran medida de que las empresas privadas que suministran servicios esenciales lo hagan de manera fiable y segura. Este punto es el clave para entender el tema del llamado "ciberterrorismo", se basa en la defensa e interrelación de las "infraestructuras críticas".

Todo surgió porque el Presidente de EE.UU. Bill Clinton creó en julio de 1996 la Comisión Presidencial para la Protección de Infraestructuras Críticas. Esta Comisión estaba integrada por personalidades de la industria privada, universidades y funcionarios públicos.

122

Igualmente estableció un Comité de Directores en que se integraron los ministros de Defensa, Justicia, Tesoro, Comercio, Transporte, Energía, y el Director de la CIA entre otros.

Entre los miembros de la Comisión, por mandato presidencial, debía haber representantes de CIA, FBI, NSA, Departamento del Tesoro, Comercio, Justicia, Defensa, Transporte y Energía.

En octubre de 1997 la Comisión envió el informe "Critical Foundations: Protecting America's Infrastructures" al Presidente. En este informe se definen lo que se consideran "Infraestructuras Críticas" como "aque- llos sistemas, cuya inhabilitación o destrucción produciría un debilitamien- to en la defensa o en la seguridad económica de la nación. Se incluyen tele- comunicaciones, energía eléctrica, gas, combustibles, sistemas bancarios y financieros, transporte, suministro de aguas, servicios gubernamentales y servicios de emergencia". Asimismo se define como amenaza " cualquiera con la capacidad, tecnología, oportunidad e intención de causar daño. Potencialmente las amenazas pueden ser domésticas o internacionales, internas o externas, patrocinadas por otro Estado o por elementos incon- trolados. Se incluye a terroristas, personal descontento propio, camuflados y hackers."

En general el informe vino a ratificar la increíble dependencia de estos sectores críticos de los ordenadores y de las comunicaciones entre los mismos. Al mismo tiempo se ratificaba que tareas gubernamentales, como Defensa, dependían cada vez más de servicios proporcionados por el sector

privado (combustibles, electricidad, etc.) por lo que la conclusión final era que la seguridad nacional, ahora más que nunca, no depende exclusivamente del Estado, debe también participar activamente el sector privado.

Influido por este informe en mayo de 1998 Clinton nombró un Coordinador Nacional de Seguridad, Protección de Infraestructuras y Contraterrorismo. En junio del mismo año, ante el Congreso, Clinton anunció la creación de la Oficina para el Aseguramiento de Infraestructuras Críticas (CIAO), dependiendo directamente del propio Presidente. Previamente, en febrero de 1998, como consecuencia de una orden presidencial el Departamento de Justicia crea el Centro Nacional de Protección de Infraestructuras (NIPC), el cual se ubica en la sede central del FBI y se compone de agentes federales de diversas agencias, representantes de los servicios de inteligencia y de las empresas privadas, con la misión de realizar análisis de amenazas e investigaciones sobre los casos que pudieran producirse.

Después de los ataques del 11 de septiembre de 2001, el Presidente Bush creó el Ministerio de Seguridad Interior (Department of Homeland Security) integrando a 22 agencias de seguridad e inteligencia que anteriormente estaban integradas en numerosos ministerios. El Centro Nacional de Protección de Infraestructuras Críticas (NIPC) y la Oficina para el Aseguramiento de las Infraestructuras Críticas (CIAO) pasaron a depender de este nuevo Ministerio, al igual que el Centro Federal de Respuesta a Incidentes Informáticos (FedCIRC), unificando bajo un sólo ministerio todo lo relacionado con la seguridad informática, al menos en terreno civil.

123

La dependencia e influencia de los ordenadores es tal que incluso ha cambiado conceptos muy arraigados en la planificación y actuación de la defensa. Lo que antes se conocía como C3 (Command, Control and Communications) ahora, por influencia directa de lo que supone la informática se ha convertido en C4I (Command, Control, Communications, Computers and Intelligence). Ello nos hace vislumbrar la importancia vital que los ordenadores tienen en facetas vitales para la sociedad y los Estados.

Hoy en día los servicios básicos están regulados por medios informáticos. El propio desarrollo industrial hace que esta situación sea más cierta cada día que pasa. Los avances tecnológicos van siempre en el mismo sentido: aumentar la dependencia de los servicios de los sistemas informáticos. Los sistemas aislados son cosa del pasado, para que sean eficaces tienen que estar interconectados, comunicarse entre ellos, y compartir información. Ello les hace vulnerables.

Además los servicios son interdependientes, dependen del funcionamiento correcto entre ellos para su propia actividad. Un ejemplo típico sería la dependencia entre los sistemas eléctricos, los sistemas financieros, y



los sistemas telefónicos. Un ataque informático contra la red de ordenadores que regula los sistemas eléctricos, haría que la electricidad dejara de funcionar, caerían los sistemas de comunicaciones entre ellos, y además traería el caos a los sistemas financieros que dependen de la electricidad y de las comunicaciones para su funcionamiento. Lo mismo ocurriría en sentido contrario: a través de un ataque a los sistemas financieros podrían bloquearse los sistemas de comunicaciones, que a su vez harían caer los sistemas eléctricos.

Aún cuando en nuestros días cualquier mención a ataques contra ordenadores inmediatamente trae a la mente la red Internet, ello supondría una limitación clara de la realidad. Muchas de las infraestructuras pueden estar conectadas o ser accesibles desde Internet, pero la gran mayoría no lo son. Cuando se habla de ataques informáticos estos pueden ser realizados a distancia contra redes de ordenadores que están conectados entre sí pero aislados de otras redes como Internet, sin embargo para intercomunicarse disponen de "puertos" de acceso a distancia, que una vez infiltrados permiten acceder a toda la red privada. Gráficamente, estas redes, pueden describirse como un inmenso plato de espagueti.

124

No existe, como se ve, posibilidad de aislar los sistemas del exterior. Su propia eficacia y la clave de su funcionamiento radica en su accesibilidad. Así pues nos encontramos con que es posible lanzar un ataque perfectamente estructurado contra sistemas básicos sin necesidad de estar presentes en el lugar, ni siquiera en el mismo país. Los medios para ello son asequibles: basta un ordenador, un modem y los conocimientos adecuados, que además son de dominio público, y se encuentran en miles de lugares accesibles por Internet.

Por si ello fuera poco los instrumentos establecidos de investigación, respuesta, e incluso de cooperación internacional, resultan lentos o inútiles contra estos ataques. Si desde otro país un "hacker" penetra un ordenador y empieza a extraer información del mismo, la respuesta investigativa típica no es válida. En cuestión de minutos la información será robada, o los sistemas dañados. Para parar el ataque no valen los convenios internacionales de cooperación jurídica que se basan en las comunicaciones lentas y formales de otros tiempos y que como mucho servirían para la investigación posterior al hecho. Hoy en día la cooperación internacional en estos temas se está produciendo de buena fe, pero sin marco legal que la cubra.

Pero ¿cuáles son esos servicios básicos?, ¿esas "infraestructuras críticas" que están interrelacionadas? Los grupos varían de experto a experto, incluso de país a país, pero lo más generalmente aceptado son los siguientes grupos:



- Información y Comunicaciones. Redes de ordenadores y de telecomunicaciones transmisoras de voz y datos. Productores de software y procesos de datos.
- Sistemas de energía eléctrica. Estaciones generadoras de electricidad. Redes de transmisión y distribución que crean y distribuyen electricidad al usuario. Se incluye en esta categoría la distribución y transporte del carburante necesario.
- Producción, almacenamiento y transporte de carburantes. Incluye gas natural, petróleo en bruto o refinado y sus derivados. Las instalaciones de refinamiento y abastecimiento y sus conducciones, gasoductos, oleoductos, redes de transporte por carretera, barco o aéreo de estos productos.
- Sistemas bancarios y financieros. Organizaciones comerciales de cualquier tipo. Instituciones financieras de inversión. Instituciones bursátiles o similares. Instituciones gubernamentales, comerciales o privadas dedicadas a las transacciones monetarias, incluidos los bancos y otras instituciones de ahorro.
- Transporte. Incluye todas las redes necesarias para el funcionamiento y bienestar de la nación, tanto en términos económicos como de defensa. El espacio aéreo, líneas aéreas, aviones y aeropuertos; red de carreteras y autopistas; camiones y vehículos privados; puertos, vías marinas y acuáticas y las embarcaciones navegando por ellas; medios de transporte de masas, tanto trenes como autobuses; red de distribución de gas, petróleo y sus derivados.
- Sistemas de abastecimiento de aguas. Todos los sistemas de obtención de aguas, reservas y sistemas de almacenamiento, filtración, limpieza y tratamiento de aguas, sus redes de distribución, enfriamiento u otros mecanismos necesarios para su uso doméstico o industrial, incluyendo los sistemas de emergencia y de lucha contra incendios.
- Servicios de emergencias. Todos los sistemas de emergencia médica, policial, contra el fuego y de rescate, así como su personal.
- Servicios gubernamentales esenciales. Todas aquellas necesidades que el Gobierno tenga para el cumplimiento de su función de proveer servicios esenciales al público.

Ya conocemos los objetivos, los grupos de objetivos posiblemente interrelacionados, pero ¿quién puede atacarlos? y ¿porqué?, debemos dilucidar si una definición tradicional de terrorismo sirve para explicar qué

actos son o no son actos de ciberterrorismo. Es cierto que tradicionalmente la violencia que practican los terroristas es de carácter físico y en un mundo virtual lo "físico" aparece cuando menos desvirtuado, pero no es menos cierto que virtualmente es posible cometer casi cualquier acto de violencia física con un ordenador. El problema radica en establecer cuándo podemos hablar de "actos terroristas" en un espacio telemático y distinguirlos de "actos que causan terror" en el mismo espacio.

El FBI utiliza la siguiente definición de ciberterrorismo "cualquier ataque premeditado, políticamente motivado contra sistemas de información, sistemas informáticos, programas de ordenador y datos del que se deriven actos violentos contra objetivos civiles causados por grupos nacionales o agentes clandestinos"; para distinguirlos de otros actos vandálicos explican que "a diferencia de un virus maligno o un ataque informático que produzca una denegación de servicio (DOS) un ataque ciberterrorista se realiza para causar violencia física o un daño económico extremo".

126 Quizás esta definición no sea perfecta, es posible incluso mejorarla añadiendo la motivación religiosa y/o nacionalista, y aún más incluyendo el deseo de obtener ventajas con la violencia y/o la intimidación sobre un sector social, pero al menos establece una separación clara entre el vandalismo o gamberrismo y el terrorismo, y ello es de agradecer especialmente al hablar de algo tan lejano, mitificado y desconocido como el ciberterrorismo. Vemos pues que para que una acción o acciones puedan calificarse de "ciberterrorismo" los requisitos a cumplir son numerosos y más o menos coinciden con los que se requieren en el mundo real y tangible. Observamos también que los actos que más preocupación causan en los medios de comunicación y por traslación a la propia sociedad son los posibles actos realizados por "cibergamberos". Ello no quiere decir que esos actos de vandalismo cibernético carezcan de peligro, lo tienen y mucho, simplemente quiere decir que tenemos que mirar en muchas direcciones para investigar los posibles atacantes y sus motivaciones.

En alguno de los siguientes grupos se pueden incluir a casi todos los posibles atacantes:

- Aficionados al ordenador que por alguna razón misteriosa encuentran excitante el penetrar en otros ordenadores en los que les está prohibido entrar. Generalmente no son malignos y no producen daño intencionalmente. Se conforman con hacer pública su "heroicidad" por haber conseguido penetrar.
- "Hackers" malignos. Realizan las mismas penetraciones pero con intención de hacer daño a los sistemas. Se suelen autodefinir como "cyberpunks" generalmente (una especie de acratismo tecnológico que se describe en la magnífica novela "Neuromancer" de William



Gibson). Estos individuos son generalmente los autores de la mayoría de los virus y caballos de troya circulando por Internet. Pueden llegar a estar sumamente especializados como los llamados "phreakers" cuyo objetivo es controlar "la red de las redes" es decir, los sistemas telefónicos ya que consideran que quien controla estos sistemas es el dueño y señor de Internet.

- Criminales informáticos. Generalmente especialistas informáticos dedicados al delito. Su motivación es económica. Penetran sistemas y los manipulan para obtener beneficios. También pueden sustraer información propiedad de las empresas para revenderla posteriormente. No buscan ni desean notoriedad, su éxito radica en el anonimato. Este tipo es el que utilizan las grandes organizaciones criminales para el lavado de dinero.

- Antiguos empleados, o empleados enfadados con la empresa. Una gran cantidad de los daños que sufren empresas en ataques informáticos, o la sustracción y posterior venta de información propiedad de la empresa se produce por los propios empleados. Este tipo de personas aparecen frecuentemente como colaboradores estrechos de espías industriales y de agentes de inteligencia extranjeros que los utilizan para sus propios fines. Se les puede considerar el agente con más potencial dañino y contra quienes es más difícil la defensa.

- Espías industriales. Su objetivo es obtener información propiedad de las empresas para su utilización por otra empresa que les paga. También se realiza este tipo de espionaje por Agencias de Inteligencia de gobiernos extranjeros para obtener beneficios para las empresas propias del país. Quienes materialmente realizan los actos pueden ser individuos de alguno de los grupos anteriores contratados específicamente para el tema.

- Terroristas. De momento no se han producido ataques conocidos por organizaciones terroristas utilizando estos medios, pero no cabe duda de que es cuestión de tiempo antes de que descubran las facilidades a su disposición y el impacto que pueden obtener utilizando este tipo de instrumentos.

- Inteligencia. Todos los gobiernos del mundo están interesados en saber lo que se cuece realmente en otros países. Sus agencias de inteligencia no serían tales si no aprovechan estos medios de penetración en ordenadores para sus propósitos de recolección de información. Pueden utilizarse para estos fines a individuos descritos en los tres primeros apartados. Ya en 1988 la KGB pagó en cocaína a unos "hackers" alemanes para que penetraran los ordenadores de los



Laboratorios Livermoore de EE.UU. y obtuvieran información sobre el sistema antimisiles conocido como "guerra de las galaxias".

- Guerreros Informáticos "Information Warfare". Con este término se define el uso de la informática como medio de guerra por un país contra otro. Los ataques pueden ser abiertos o encubiertos, pero la intención clara es la de causar el mayor daño posible e interrumpir el normal funcionamiento de los servicios. Se trata de gobiernos dedicados al tema y por tanto los medios disponibles pueden ser cuantiosos y especializados, desde técnicas indetectables de destrucción de componentes electrónicos como el HERF (High Energy Radio Frequency), pasando por manipulaciones de procesadores o componentes de los ordenadores que actuarían cuando reciban una instrucción especial, al uso masivo de "hackers" que hagan aparecer los ataques como algo inconexo con el verdadero lanzador del ataque.

Desde que -después de los criminales ataques realizados el fatídico 11 de septiembre de 2001- Osama Ben Laden recomendaba a sus seguidores los ataques a "los objetivos económicos porque la economía es la sustentadora del poder militar", la posibilidad de que se produzcan actos de ciberterrorismo se ha tomado muy en serio en los países occidentales, y más si observamos detenidamente el perfil de muchos de los seguidores de Ben Laden. No se trata de individuos con escasa cultura y formación, se trata de fanáticos con formación universitaria, generalmente de carácter técnico y preparados en universidades occidentales, la informática no es precisamente una desconocida para ellos.

Después de haber analizado la posibilidad de realizar este tipo de ataques, de haber mencionado que pueden llegar a ser devastadores y alterar el funcionamiento mismo del Estado e incluso de la defensa de un país, nos queda por examinar un elemento fundamental y raramente examinado en este caso: la probabilidad del ataque.

Examinemos una supuesta matriz en la que se contemplen por grupos de infraestructuras:

1. Los parámetros de la probabilidad del ataque.
2. El daño que se puede causar.
3. Los conocimientos necesarios para efectuar un ataque exitoso.

Observaríamos cómo las probabilidades de ataque y el daño que se puede causar varían enormemente por grupos siendo los más perjudicados y más fácilmente atacables los sectores de Información y Comunicaciones,

y el de sistemas bancarios y financieros. Estos dos grandes grupos dependen en mayor medida de la existencia de conexiones masivas y accesibles desde cualquier punto (piénsese en el sector bancario por un lado y en las empresas de telecomunicaciones por otro). En estos dos sectores la probabilidad del ataque y el daño que se puede causar es alto, sin embargo en los otros grupos la probabilidad de éxito es baja (se necesita una gran especialización y medios) aunque el daño a causarse pueda ser alto.

Existen en la actualidad dos corrientes contrapuestas de opinión:

1. Las infraestructuras críticas son tremendamente accesibles, es fácil, y económicamente muy viable, causar mucho daño con poco conocimiento, escasos medios y con casi total impunidad.

2. Se ha exagerado enormemente el papel de las telecomunicaciones en la protección de las infraestructuras críticas. Se acepta que pueden ser susceptibles de sufrir ataques, igualmente se acepta la interrelación entre ellas, pero se añade que salvo en casos muy concretos el posible atacante necesitaría grandes conocimientos informáticos para pasar las defensas establecidas y el daño que se pudiera causar sería fácilmente subsanable.

Como casi en todo, quizás sea en un término medio donde radique la aproximación más acertada al problema que exponemos. Ni es tan fácil crear un caos económico social en un país atacando únicamente con ordenadores a redes informativas como unos piensan, ni es tan difícil y costoso como los otros exponen.

Unos exageran y solicitan grandes medios económicos para proteger redes que ya están bien protegidas.

Otros minusvaloran la capacidad e inteligencia de los posibles atacantes, echándose en manos de sus medios técnicos para impedir el acceso (cortafuegos, redes internas, etc.) olvidando que el arma más importante de un "hacker" sigue siendo la "ingeniería social", es decir, la capacidad de acudir al engaño para conseguir las claves y accesos necesarios sin preparación técnica de ningún tipo, es más, aprovechando la falta de preparación técnica de la mayoría de los empleados de las compañías.

Ya hemos mencionado que son los empleados disgustados con la empresa los atacantes más peligrosos pues ellos conocen las claves, distribuciones, etc. Imaginemos ahora por un momento si alguno de los empleados está motivado, intimidado o sufre cualquier otro tipo de influencia por un grupo terrorista o por un grupo de criminales organizados. El panorama cambia radicalmente.

Respecto al daño que puede causarse, tampoco conviene minusvalorarlo, en algunos tipos de industrias el abrir las compuertas de una presa



o el provocar un corte de electricidad o una subida de tensión puede tener consecuencias catastróficas, no digamos el mezclar el cloro en proporciones no adecuadas en las plantas de tratamiento de aguas.

Por todo ello la mejor solución es la medida y la moderación, estar alerta y conocer el riesgo, ya venga de acciones individuales realizadas por cibergamberos, por grupos organizados o por grupos terroristas. Establecer y revisar las políticas de seguridad interna de las empresas y sobre todo por la cooperación sincera, efectiva y confidencial de las empresas privadas y la Administración, reconociendo que es un problema que afecta a ambos y que únicamente trabajando juntos se puede atajar.

Los ataques que se han producido hasta la fecha siempre han sido realizados por cibergamberos. En algunos casos se han detectado ataques contra los sistemas económicos y bancarios realizados por grupos de delincuencia organizada, siempre orientados a obtener beneficios económicos o a camuflar el origen ilícito del dinero que mueven. Las acciones de grupos terroristas en el llamado ciberespacio se han limitado hasta la fecha al proselitismo y al uso del mismo para efectuar comunicaciones seguras entre miembros del grupo utilizando programas de cifrado y de ocultamiento como PGP y la esteganografía. Cuando se ha producido una incidencia de carácter informático importante ha sido precisamente porque una acción terrorista física ha dañado las redes lógicas (por ejemplo, la caída de las torres gemelas dañó el sistema informático de Wall Street).

130

Lo más importante es destacar que tanto la Administración como las propias empresas privadas son plenamente conscientes del problema y toman medidas preventivas para que no se produzcan incidencias en este terreno. Conocer el problema es sin duda el primer paso para la prevención del mismo, por ello es vital que la Policía pueda contar con los medios técnicos y con los medios jurídicos que posibiliten la investigación de toda incidencia que se produzca. El derecho al anonimato no puede significar el derecho a la impunidad. La posibilidad de investigación de estos ataques, y por consiguiente de su persecución judicial, es fundamental para que los mismos no se produzcan.



## **CIBERESPACIO Y DELINCUENCIA ORGANIZADA**

**Francisco Aranda Guerrero  
Comisario del Cuerpo Nacional de Policía  
Jefe de la Oficina Central Nacional de Interpol  
(INTERPOL Madrid)**

131

Abordar una materia de esta naturaleza, plantea siempre de inicio una cierta duda, es decir si nos encontramos ante una temática o conjunto de elementos de nuevo cuño para la humanidad su estructura social y de comportamiento, o por el contrario se trata simplemente de un proceso evolutivo más en la larga marcha de los tiempos, hoy en el planeta tierra, mañana Dios sabe.

Hecha esta pequeña reflexión inicial que luego profundizaremos, convendría pasar inmediatamente a la consideración de conceptos. Si acudimos a una definición técnica, probablemente la de Barlow sería válida perfectamente, su idea de considerar el ciberespacio como "...el lugar que se crea entre ordenadores, redes y la información en ellos contenida..." No obstante y dado que siempre es aconsejable consultar la opinión popular y dentro de ésta la de los mayores consumidores potenciales de informática, es decir los más jóvenes; algunos muestreos llevan al convencimiento de que para ellos el ciberespacio es "...algo muy grande que está ahí pero que no se toca..."

Dicho lo cual cabría entrar en la segunda parte, es decir la idea de delincuencia organizada. Resulta evidente que en la misma se comprenden principios como planificación, asesoramiento, infraestructura y recursos, por tanto todo hecho delictivo que comprende tales principios, a los que se une por razones obvias la existencia de grupo de personas, en sentido quizá comparable a aquel viejo y romántico concepto empleado en los códigos penales de cuadrilla.

La inmensa mayoría de las figuras penales vigentes, exceptuando las pasionales y algunas específicas, pueden ser cometidas en modalidades de delincuencia organizada, ya que desde las falsificaciones, a los grandes tráfico, pasando por el terrorismo, no son sino modalidades diversas de delito organizado, en contra de las separaciones que suelen hacerse, especialmente respecto de este último, que debería ser pura y simplemente considerado como una forma más de delincuencia organizada, evitándose así diferencias entre delincuentes que a veces inciden negativamente respecto de los conceptos de justicia.

De esta manera nos encontramos con que grupos organizados utilizan el ciberespacio como medio para cometer sus hechos delictivos o al menos como territorio de apoyo útil y específico para alcanzar el logro de estos. Evidentemente el concepto de grupo alcanza desde los pequeños y especializados hasta las grandes organizaciones internacionales, fluctuando entre quienes tienen como elemento esencial el ciberespacio para la ejecución, por ejemplo transferencias bancarias fraudulentas, hasta los que se sirven del mismo como sistema auxiliar de gran poder, esencial pero colateral al delito, por ejemplo comunicaciones vía Internet entre traficantes de drogas para sus transportes y citas, en todo caso, ambas tienen en común idéntico medio.

132

Establecido lo anterior habría que considerar si la ciberdelincuencia no es en realidad más que un fenómeno fruto de un proceso de adaptación al medio por parte de los delincuentes, consecuente con el propio principio de la evolución delictiva y que "arrastra" como motor a parte de su entorno, es decir el nacimiento lógico del ciberespacio es víctima de la idea de rentabilidad criminal del delincuente, el cual lo utiliza para el logro de sus fines y/o como herramienta, lo que nos llevaría entonces a considerar que se ha producido una nueva implantación y asentamiento de tecnología, muchas veces a los niveles más avanzados, entre los autores de los delitos y estos mismos como fin último.

Evidentemente la apertura de Internet y todo lo que rodea la cibernética en general, ha supuesto además de la lógica vía de progreso en sus relaciones de diferente naturaleza para millones de ciudadanos en el mundo, el acceso también de los delincuentes en su conjunto y específicamente de los grupos organizados a una gran ventana, que llega por primera vez desde la época feudal a situarles en algunos casos a nivel de enfrentarse a gobiernos y Estados, haciéndoles pasar a estos últimos amargas horas como recientemente se ha puesto de manifiesto, pero no sólo a los Estados, sino también a los ciudadanos individualmente o como colectivo, los grupos de delincuentes convenientemente "tecnologizados" cargan sobre ellos sin piedad alguna continuos hechos delictivos de diferente naturaleza pero con idéntico sujeto pasivo.

## **INFORMACIÓN: SU IMPORTANCIA COMO RECURSO ESTRATÉGICO EN UN MUNDO GLOBAL Y TECNOLOGIZADO**

Si es cierto que cualquier grupo de delincuentes de medio pelo cuenta hoy con asistencia financiera, legal y tecnológica, lo es tanto o más que la información es un elemento esencial en nuestra sociedad, imprescindible para el delincuente y más imprescindible si cabe, para la lucha contra el delito.

Considerando que las dos grandes fuentes de información son las humanas y las tecnológicas y aunque detrás de las segundas están siempre las primeras, el ciberespacio ha supuesto un caudal ingente de información, que convive con el viejo concepto de fuentes abiertas y cerradas, aumentando ingentemente las posibilidades de las primeras y técnicamente el alcance y calidad de las segundas, creando grandes dificultades para el control y procesado del volumen información y abriendo un inmenso mundo de posibilidades a la sociedad en general y a los delincuentes en particular.

Todo este conjunto debe inscribirse en un mundo globalizado, en el que la, en su momento, innovadora imagen del joven sobre un borrico con un fusil y un tremendo radiocassette japonés al hombro, ha dejado paso a la del traficante o el terrorista dotado de teléfono satelital, ordenador portátil conectado y capacidad de desplazarse de un lugar a otro tejiendo redes delictivas, por tanto el concepto de globalización es otro elemento más, con una faceta de potenciador de la ciberdelincuencia o cuando menos intrínsecamente utilizable por ésta.

133

## **LA UTILIZACIÓN DE LAS VIEJAS Y NUEVAS TECNOLOGÍAS**

Partiendo de la base de la continua evolución y adaptación al medio de la delincuencia organizada en relación con el ciberespacio, cabría considerar tres posibles niveles posicionales:

a) Viejas técnicas ejercidas sobre nuevas actividades delictivas: en este conjunto cabría enmarcar la violencia tecnológica contra las actividades de entidades financieras, empresas, etc, con el fin de privarles fraudulentamente de los recursos que gestionan, lo que podríamos llamar la vieja técnica del atraco realizada contra la actual actividad económica tecnológica, en vez del clásico a mano armada.

b) Nuevas técnicas ejercidas sobre actividades tradicionales: consideraríamos el lavado de dinero, la captación de información útil, sobre objetivos, lugares, personas etc., así como la difusión de informaciones



interesadas a favor o en contra de lo que fuere, mediante la cibernética y los medios que esta proporciona, validos por ejemplo para movimientos de capitales, gestión de sociedades interpuestas u otras figuras.

c) Nuevas técnicas ejercidas sobre nuevas actividades: agresiones técnicas digitales para penetrar en modernas bases de datos o destruir éstas dañando su utilidad o lo que representan, incluyendo entre otros posibles valores añadidos como la rentabilización de la publicidad del acto en una sociedad en la que influye plenamente la información y la informatización.

Los antedichos modelos clasificatorios tienen en común el impacto que esta evolución tecnológica materializa en la delincuencia organizada, su constante adaptación al medio y la real dependencia de la sociedad actual respecto de los ordenadores y las redes, junto con las vulnerabilidades que estos tienen.

Esa vulnerabilidad es sin duda un hecho contrastado, que siendo constante motivo de preocupación para quienes actúan en la legalidad, es reto permanente para quienes tratan de rentabilizarla ilícitamente en su beneficio, llegándose a la paradoja de contratar personas salidas del mundo delictivo como medio para defenderse de agresiones tecnológicas, dentro de la constante innovación del delincuente y la entrada en los grupos organizados que utilizan estos recursos, de nuevos individuos con formación suficiente, que se desvían de la ética profesional, atraídos por los beneficios a conseguir, es decir la preponderancia de la oportunidad sobre cualquier otro principio de conducta.

## LAS MODALIDADES DELICTIVAS

Se ha dicho ya que esta adaptación al ciberespacio se ha realizado profundamente y continúa tanto en la sociedad globalizada como en la delincuencia organizada, por tanto aunque en menor escala, desde las figuras delictivas más comunes hasta las más sofisticadas, los autores de todas ellas se han adaptado a las nuevas tecnologías y continúan haciéndolo, no obstante deben resaltarse algunas modalidades que por su presente y su previsible evolución merecen este tratamiento.

La romántica figura de los piratas informáticos, "hackers", y rompedores de códigos, que ha promovido actividades tan "populares" como la falsificación de tarjetas codificadas para televisión de pago, telefónicas y un sin fin de variedades, muchas de las cuales siguen en auge de consumo especialmente en países de menor desarrollo, o producen cantidades ingentes de falsificaciones mediante copias informáticas fraudulentas musicales, de vídeo, juegos, programas, etc. encontrando un cierto eco de justificación moral debido a los altos precios de comercialización.

Las guerras entre cibernautas de grupos o países enfrentados, han incrementado su tecnología, capacidades y virulencia, fijando objetivos más altos, cambiando escrúpulos por intereses y desarrollando virus informáticos cada vez más eficaces en su labor destructiva.

En este sentido debe considerarse también el carácter pluriactivo del crimen organizado, que lleva a los autores no sólo a la planificación y ejecución de hechos delictivos, muchas veces de distintas modalidades, sino además a la comercialización de los frutos obtenidos, gestión de los recursos generados y sostenimiento de la organización junto con las necesidades de sus miembros.

En tal contexto son los delitos de naturaleza económica considerados fin último, como aquellos en que es colateral, (blanqueo- tráfico de drogas), los que van a seguir teniendo un papel creciente.

A ello hay que unir sin duda las falsificaciones, tanto de todo tipo de documentos identificativos, como de dinero títulos o cualquier otra modalidad de bienes y su gestión, sin olvidar el "repicado" de tarjetas de crédito u otros medios de pago, todo ello sirviéndose de las nuevas tecnologías, tanto para la obtención o elaboración del documento como para su uso.

135

Junto a ellos y a los ya clásicos pero adaptados tráficos de drogas, armas y seres humanos, debe considerarse con carácter de importancia el fenómeno terrorista en un planeta en el que seguirán coexistiendo múltiples conflictos focalizados, que entre otras cosas llenan el ciberespacio de páginas de grupos y grupúsculos que buscan difusión y apoyo, sirviéndose igualmente de la "web" para sus contactos y operaciones.

En este sentido se entremezcla la delincuencia organizada de distintas modalidades bajo el epígrafe de la rentabilidad, así mientras el terrorista sueña con acceder a posibilidades destructivas que pongan bajo su pie a ciudadanos y gobiernos, el traficante organizado esta dispuesto a intentar conseguir todo aquello que pueda vender a altos precios y sin escrúpulo alguno, esta conjunción se pone de manifiesto y adquiere importancia y volumen creciente cuando se trata del llamado material industrial de doble uso. Las sustancias radiactivas, parte de las cuales han dejado de estar bajo control de la autoridad que las custodiaba como consecuencia de la desintegración de estructuras de Estados anteriores, así como las de nueva manufactura y los equipos necesarios para obtenerlas, son objeto codiciado de demanda para el tráfico, llegando incluso a producirse situaciones picarescas de estafa entre grupos vendedores y compradores.

No debemos olvidar el auge y relevancia creciente del espionaje industrial, en un mundo como el actual en el que se mueven grandes flujos económicos e intereses al socaire del tejido empresarial.



Ya no se trata sólo de acceder al desarrollo de nuevos productos sino de hacerlo en una posición de primacía, por tanto el ciberespacio y la tecnología que lo rodea constituyen entorno y medio ideales para este tipo de delincuencia organizada, en el que corren parejos la presión tecnológica delictiva y la demanda de este tipo de actuaciones, en función de la rentabilidad que se deriva de poseer o no poseer tales activos.

La pornografía infantil y todo lo que rodea la llamada sexualidad clandestina, especialmente dirigida contra menores de ambos sexos, se ha convertido en un creciente mercado que mueve ingentes cantidades de dinero, teniendo numerosos seguidores en la web, además de los que utilizan ésta como vehículo de gestión para sus operaciones, (turismo sexual, extorsiones, etc.), no debiendo obviarse tampoco la obtención de información para otros delitos, a partir de tales prácticas.

Sería igualmente oportuno mencionar la importancia de la "web" para la difusión de técnicas innovadoras en el ámbito delictivo, aquí cabe citar como ejemplo entre otros la difusión de los sistemas hidropónicos para el cultivo de estupefacientes, los métodos de elaboración de drogas sintéticas, explosivos, ruptura de códigos de seguridad y un largo etcétera.

136

El perfil tanto de los grupos como de los individuos responde cada vez a una mayor formación cultural/tecnológica de sus miembros en relación a los fines perseguidos, en ciertos casos instrucción especializada previa adquirida en centros militares, estatales o de investigación, que redundan en superior planificación, mejor sostenimiento de estructuras y fijación de objetivos más altos y rentables, junto a una mayor ausencia de escrúpulos.

Al crecimiento y evolución de este conjunto habrá que hacer frente de una manera adecuada en el futuro inmediato.

## LA LUCHA CONTRA ESTE TIPO DE DELITOS

Si hemos dicho que la sociedad en general ha evolucionado alrededor del ciberespacio y la globalización y dentro de ella la delincuencia organizada, otro tanto ha sido y es preciso hacer desde el lado de la ley y el orden, es cierto que la investigación policial va generalmente detrás de los avances de los grupos de delincuentes, pero no es menos evidente que aunque se ha producido también una adaptación por parte de los servicios policiales, urge proseguir por ese camino quemando etapas.

Es poco lo que puede hacerse sin contar con tres factores esenciales:

a) Normativa legal adecuada. Las importantes dificultades con que se encuentran los investigadores respecto de entes como los paraísos fisca-



les y prácticas como las sociedades interpuestas, se ven agravadas en el ciberdelito por la ubicación de servidores en lugares remotos que permiten la utilización, cuando menos temporalmente, impune para sus fines y especialmente el grado de anonimato que confiere actuar a través de Internet, de manera que basta una simple conexión desde un cibercafé, o el equipo y conocimientos adecuados, de lo cual no están faltos los grupos organizados, para realizar desde amenazas o extorsiones hasta un largo etcétera de figuras delictivas.

No es preciso decir que este tipo de delincuentes tiene asesoramientos suficientes que acuden en su auxilio si se produce la detención, mientras el investigador sigue encontrándose en un entramado de dificultades, el cual se ve agravado ante la no tipificación, proteccionismo, disparidad o falta de homogeneidad, aunque sólo fuera en lo esencial, existente en muchos lugares sobre los que cuesta creer que la ciberdelincuencia aplicada a la actividad económica delictiva y al blanqueo de capitales no es una industria más. Normas como el Convenio de Budapest de 2001 y otras no se han revelado como suficientes para la prevención y lucha.

b) Formación continuada para los investigadores. La formación continuada de los investigadores, junto con la captación de expertos en la materia para el ingreso en la actividad policial y la continuidad en la tarea durante un periodo de tiempo rentable para todos, son factores primordiales, equilibrando las plantillas en una correcta proporción de veteranía y experiencia que conjuntan savia nueva, nuevos conocimientos y relevo generacional, es algo imprescindible también para el logro de buenos resultados. Precisamente por ello los formadores deben ser siempre profesionales en régimen de actividad habitual relacionada con la especialidad delictiva, de diferentes extracciones profesionales y distintos enfoques, todos ellos absolutamente prácticos.

c) Disposición de la tecnología necesaria. De nada serviría todo el esfuerzo humano y de normativa si no se dispusiera de la cantidad y calidad de equipamiento de "software" y "hardware" suficiente, de igual manera que un buen jinete sirve de muy poco sin un buen caballo, el investigador necesita junto con el respaldo legal adecuado, contar con la tecnología que le permita luchar dignamente contra estas formas de criminalidad, únicamente bajo el imperio de la ley y con las premisas antedichas es posible combatir eficazmente esta problemática, evitando al tiempo la sensación de "solo ante el peligro" en que a veces se encuentran los investigadores, los cuales deben disponer al menos, de similares sistemas interactivos a los que usan los delincuentes.

## CONCLUSIONES

a) Desde el punto de vista policial:

- Crecimiento de la presencia de este conjunto integrado por delincuencia organizada y ciberespacio.
- Más que de nuevos delitos podría considerarse como adaptación al medio a partir de novedosas herramientas y tecnologías en continuo de sarrollo y progreso.
- La importancia de la publicidad en algunos tipos de estos delitos y el aumento de impunidad y rentabilidad que proporcionan.
- La potenciación de instrumentos como la Orden Internacional de Busca y Captura conjuntamente con la Orden Europea, las entregas temporales para interrumpir prescripciones, las Comisiones Rogatorias Internacionales y mayores facilidades para la investigación al tiempo que se eliminan barreras proteccionistas para lograr una mejor y más equitativa administración internacional de la justicia.

138

b) Incidencia de factores sociales:

En una sociedad tan globalizada como la actual en la que los medios de comunicación facilitan el conocimiento de desarrollos y formas de vida y en la que no necesariamente los expertos proceden de países desarrollados, basta ver el número de paquistaníes que trabajan en empresas informáticas, se están produciendo cambios económicos y sociales continuos e importantes.

- Inflación. La economía de muchos países de la tierra carece de tejido industrial e infraestructuras, exceptuando la comercialización de materia primas como el petróleo, los que lo poseen, a lo que se une una corrupción endémica en bastantes casos.
- Crecimiento demográfico desbordante. Una de las constantes más habituales en los Estados con mayores problemas económicos es el aumento incontrolado de población, mientras se produce una reducción de la natalidad en los desarrollados, al tiempo que aquellos se encuentran carentes de imprescindibles servicios sociales y laborales, lo que coloca a muchas personas al borde de la desesperación y en la indigencia, lo que es aprovechado para crímenes como la explotación de seres humanos y otros.
- Fanatismo violento. La ausencia de principios democráticos en buen número de países junto con la existencia de dictaduras de

cualquier signo y la pérdida de principios ideológicos arraigados socialmente en el pasado, han permitido en su conjunto y en conexión con los otros factores sociales antedichos el crecimiento de formas violentas y fanáticas que hábilmente dirigidas por individuos con personalidades mesiánicas, sin moral racional e inteligentes, favorecen la proliferación de delitos de todo tipo, convirtiendo a miles de personas en autores y/o víctimas de actos criminales.

Por ello faltaría un elemento importante, si no se significara al concluir que también los factores sociales tienen igualmente su incidencia en las actividades de la delincuencia organizada y en el ciberespacio, precisando una atención adecuada por parte de los organismos supranacionales y los Estados, especialmente si se desea evitar o cuando menos reducir la incidencia de dichos factores y por tanto el volumen de delincuencia global existente.



# **LA DELINCUENCIA VIRTUAL EN LA UNIÓN EUROPEA. VALORACIÓN Y EVOLUCIÓN DEL FENÓMENO**

**IAN CASEWELL**  
**Analista de Europol**

**141**

La delincuencia cibernética está rodeada de un velo de misterio, debido a la propia naturaleza de estos delitos: el hecho de que estos pueden producirse y, de hecho, se producen dentro del "cibespacio". Delitos en los que están implicados predominantemente unos datos y una información, que son los productos intangibles del delito. También deberá tenerse en cuenta que la delincuencia informática no es, con frecuencia, un hecho aislado sino un delito que forma parte de otro que ocurre también dentro del mundo físico. Es muy difícil encontrar un delito del mundo real que no tenga ningún elemento de alta tecnología, aunque sea algo tan común y sencillo como la utilización de un teléfono móvil. Esta es quizás la razón por la cual el término delincuencia cibernética no es el término apropiado para reflejar el trabajo que los Cuerpos de Seguridad han realizado en los Estados miembros y el de delincuencia de alta tecnología quizás encajaría más fácilmente.

De acuerdo con el trabajo que Europol ha realizado en este campo, se utilizan las siguientes definiciones:

- Delincuencia de alta tecnología. El uso de la información y de la tecnología de las comunicaciones con el fin de cometer o promover un acto delictivo contra una persona, propiedad, organización o sistema informático de trabajo en red.

- Delincuencia cibernética. Uso de redes de ordenadores o sistemas en Internet con fines delictivos. Ataques contra sistemas y redes o uso indebido de los mismos con fines delictivos. Delitos y uso indebido, ya sea por parte de delincuentes que actualmente utilizan nuevas tecnologías como nuevos delitos que se han desarrollado con el crecimiento de Internet.

Los ordenadores e Internet son otra herramienta que se añade al arsenal que los delincuentes tienen a su disposición para cometer delitos. Un buen comienzo para entenderlo es realizar un acercamiento a la delincuencia informática.

### **VIEJOS DELITOS, NUEVAS HERRAMIENTAS Y NUEVOS DELITOS, NUEVAS HERRAMIENTAS**

Todos los tipos de delitos tradicionales pueden facilitarse y tener como soporte la Tecnología de la Información y de la Comunicación (TIC): el fraude, el robo, la extorsión, el tráfico de drogas, tráfico de seres humanos, inmigración, pedofilia, terrorismo. Los nuevos delitos son los que tienen como objetivo el ataque a sistemas y redes, como formas de piratería informática, virus y denegación de servicio (DOS). Sin embargo estos últimos tipos pueden servir de apoyo a otros delitos tradicionales como son la extorsión, el fraude y la piratería informática, para la obtención de datos que es una forma de robo. Así la distinción entre viejos delitos y nuevos puede hacerse aún más confusa. Estamos contemplando la evolución de la delincuencia hacia la explotación de los nuevos medios y ello puede exigir disponer de unas capacidades específicas de la Tecnología de la Información y de la Comunicación que faciliten la intención criminal.

La delincuencia cibernética es horizontal por naturaleza; produce un impacto en todos los tipos de delito.

### **USO Y EXPLOTACIÓN DE TECNOLOGÍA DE LA INFORMACIÓN Y DE LA COMUNICACIÓN**

Las implicaciones de la delincuencia en la era de la información pueden dividirse de forma definitiva en cuatro áreas clave si nos atenemos a las facilidades que tiene la intención criminal:

1. La Tecnología de la Información y de la Comunicación como medio de comunicación de delincuentes (Delincuencia Organizada).

Los desarrollos tecnológicos, particularmente en lo que respecta a Internet, se han sumado en gran medida a la capacidad del delincuente y

el alcance de la comunicación, la cual puede ocultarse de la Policía de muchas maneras.

2. La Tecnología de la Información y de la Comunicación para facilitar la actividad delictiva (Delincuencia Organizada).

Internet proporciona a los delincuentes un alcance a escala mundial, el anonimato, unas comunicaciones instantáneas seguras, acceso al conocimiento, más objetivos, aportándoles de esta manera una gran cantidad de oportunidades delictivas y facilidades para sus actividades actuales.

3. Los ordenadores y las redes como objetivos.

Los sistemas de información, las redes y los dispositivos de comunicación están cada vez más conectados entre sí. Esta convergencia ha aumentado las posibilidades de intrusión, manipulación, disrupción, destrucción y robo de datos. La fiabilidad de los ordenadores y redes y de los datos que pasan a través de estos ha aumentado su atractivo como objetivos.

4. La Tecnología de la Información y de la Comunicación como dispositivo de almacenamiento.

La información digital es una fuente de pruebas adicional, que puede ser un escenario del crimen en sí misma o una extensión de lugares de delitos en el mundo físico. El propio uso de la Tecnología de la Información y de la Comunicación crea archivos y registros y el almacenamiento de datos relacionados con actividades delictivas (por ejemplo, comunicación, imágenes, propiedad intelectual, archivos de empresa, herramientas de ataque, etc.) pueden resultar ser fuentes incalculables de pruebas.

143

La mayor parte de la delincuencia en Internet conlleva, de una manera u otra, la transmisión de información. Esto está relacionado con el suministro de productos ilegales, servicios e información o con la obtención de información ilegal, sea mediante robo, engaño u otros medios. Así pues, el acto ilegal normalmente representa un delito tradicional y por lo tanto está relacionado con el contenido de la información.

## VALORACIÓN DE LA MAGNITUD Y DE SU IMPACTO

Existen muchas limitaciones y obstáculos para la obtención de información fidedigna que describa y valore el volumen e impacto de la delincuencia cibernética. Esto aumenta más cuando se intenta hacer lo mismo en el contexto del crimen organizado. Existen pocos datos cuantitativos, si los hay, para la valoración del tamaño e impacto de la delincuencia cibernética dentro de la Unión Europea. La UE se resiente de la falta



de mecanismos para la captura de datos en las formas variables de la delincuencia cibernética, e incluso es un reto mayor la extracción del elemento de alta tecnología entre los delitos ya denunciados.

Tal como ha sido destacado en la investigación del Joint Research Centre of the European Commission: "un sistema de información riguroso y admisible para Europa y los Estados miembros es importante para entender la envergadura que esta amenaza representa para los ciudadanos y E-Europe"(1).

El problema de la valoración del impacto de la delincuencia cibernética está más exacerbado por la falta de denuncias y materias relacionados con las víctimas, no teniendo conocimiento de si se ha producido o no alguna infracción. Esto tiene graves implicaciones para los Cuerpos de Seguridad en cuanto a la asignación y justificación de recursos e información fiable que guíe las actividades en este campo.

Uno de los cometidos de los grupos del análisis de la delincuencia de alta tecnología en Europol, era la elaboración de una evaluación estratégica para los Cuerpos de Seguridad de la UE. Tal como se describe a continuación, hubo muchas limitaciones y se intentó solucionarlas, a través de un acceso a la información e inteligencia válida, mediante la creación de un

144

Grupo de Información Estratégica contra la Delincuencia Cibernética. Este grupo está formado por expertos de los Estados miembro de la UE dedicados al cometido de la información (inteligencia) en este campo de la delincuencia de alta tecnología.

Con la creación de un Grupo de Información Estratégica contra la Delincuencia Cibernética, se definieron los objetivos de valoración como:

- Descripción de la delincuencia cibernética y los factores que facilitan las ofertas tecnológicas a los delincuentes.
- Valoración de la amenaza de la delincuencia organizada.
- Evaluación de la capacidad de los Estados miembro para responder a la amenaza.
- Identificación de las áreas que necesitan una mayor y más profunda investigación.
- Mejor entendimiento de la amenaza.
- Desmitificación y visualización de la naturaleza horizontal.

---

1.- "Ciber abuse in E-Business Processes: Report of an Exploratory Study", Joint Research Center of the European commission, Octubre 2001.

Con el fin de cumplir estos objetivos, las fuentes de investigación identificadas fueron: estudios y entrevistas realizados con investigadores de delincuencia de alta tecnología, la provisión de estudios de casos, estudios existentes en la industria y una recopilación dirigida de datos de fuente abiertas. La investigación cualitativa, llevada a cabo mediante visitas realizadas a las Unidades de Delitos Informáticos (CCU – Computer Crime Units) de los Estados miembro de la UE, mostraba que la mayoría de estas unidades eran incapaces de manejar todos los casos que llegan a sus unidades. Esto se debe en parte a una asignación de recursos limitada y al aumento del número de incidentes y demandas. Los temas de interés que rodean las tendencias que van surgiendo y las amenazas futuras destacadas, a lo largo de esta investigación, se centran principalmente en:

- Robo de identidad como apoyo de otras formas de delincuencia.
- Uso de tecnología de banda ancha y sin cable.
- Aumento de la capacidad para el almacenamiento de datos.
- Aumento del uso de medios de comunicación sofisticados por parte de los delincuentes.
- La codificación de los canales de comunicación y el almacenamiento de datos.
- Falta de conciencia a nivel de encargados de la toma de decisiones, lo cual representa un impacto negativo en el presupuesto y asignación de recursos.
- Robo de la propiedad intelectual.
- Cuestiones sobre la conservación de datos.

145

## DETERMINACIÓN DE LA AMENAZA

Para determinar la amenaza de la delincuencia de alta tecnología es necesario observar los diferentes aspectos relacionados con las víctimas; los delincuentes; los factores que facilitan la delincuencia; la seguridad de la información; los Cuerpos de Seguridad y la capacidad de los Estados miembro para responder a la amenaza. Se puede decir, que todo lo expuesto a continuación ha aumentado y continuará aumentando con los avances de la Tecnología de la Información y de la Comunicación dentro de la sociedad:

- Facilidad de conexión.

- Alfabetización informática.
- Velocidad de carga y descarga.
- Capacidad de almacenamiento de datos.
- Gastos de comercio electrónico.
- Disponibilidad de la información y las herramientas para cometer delitos.
- Número de ataques contra las redes, sistemas, público, industria y organizaciones.
- Mayor sofisticación en los instrumentos para cometer los ataques.
- Coste de la delincuencia informática para todos los organismos.
- Centralización de las operaciones comerciales normales a través de las redes informáticas.
- Vulnerabilidades que están siendo explotadas a nivel global, poniendo en evidencia la volatilidad de la red mundial de ordenadores.

146

## OPORTUNIDADES DE LA DELINCUENCIA

Con la expansión de Internet y su aceptación por parte la sociedad, ha habido un gran aumento en el número y tipos de objetivos que ahora se encuentran a disposición de los aspirantes a "delincuentes cibernéticos". Actualmente se encuentran disponibles por todo el mundo objetivos, desde instituciones militares, gobierno e instituciones gubernamentales hasta negocios de empresas y comerciales, el público y los usuarios de los servicios de la red y las propias empresas que facilitan la infraestructura y los servicios de Internet (es decir, el robo de servicios de compañías de telecomunicación y proveedores de servicios de Internet, ataques de denegación de servicio) y objetivos importantes de la infraestructura nacional.

Internet facilita a los delincuentes un acceso a escala mundial, el anonimato, comunicaciones seguras al instante, acceso al conocimiento, un aumento de objetivos y unas abundantes oportunidades para la delincuencia, así como facilidades para actividades que ya existían. Los mercados potenciales para la delincuencia se han ampliado, así como la posibilidad de encontrarse y comunicarse con personas con sus mismas intenciones.



En general la sociedad está más informada con el uso de la Tecnología de la Información y de la Comunicación. Junto a estos progresos en la sociedad se fomenta la mentalidad delictiva, la cual se extenderá aún más por las oportunidades que existen de cometer "delitos cibernéticos".

Debido a la confianza de la sociedad en las redes informáticas y en información que se asienta y viaja dentro de ellas, ha aumentado de forma espectacular la amenaza de utilizar estos sistemas como objetivo. Las vulnerabilidades a nivel mundial de la red han venido manifestándose a través de incidentes de códigos malévolos extendidos por todo el mundo, paralizando sistemas con unos daños que cuestan millones de euros. El virus "I Love You" y los de tipo gusano como el "Code Red", el "Nimda" y el gusano "Slammer", de este año han mostrado todos ellos la inestabilidad de la red mundial. En tanto que ha aumentado la cantidad y el coste de los daños, ha disminuido el tiempo de accesibilidad más frecuente.

### ¿QUIÉNES SON LAS VÍCTIMAS?

Existen víctimas potenciales dentro de cada sector: industria, gobierno, ejército y público. Todos ellos están expuestos a la explotación de las vulnerabilidades a nivel mundial de la edad de las comunicaciones, siendo la industria el blanco más provechoso para los delincuentes, donde se ha visto un aumento importante de ataques informáticos, dirigidos a recursos de información, fraude, etc. El lento desarrollo del comercio electrónico, en contra de las predicciones iniciales de crecimiento se atribuye, en parte, a la delincuencia informática y al miedo a la delincuencia cibernética por parte del público.

La mayor parte del crecimiento de interés por el uso de Internet está en Asia, Latinoamérica y partes de Europa. A finales de 2005 el número de usuarios de Internet por todo el mundo será casi el triple, hasta unos 1,17 billones, se observará una parte cada vez mayor de estos en el uso de dispositivos sin cable(2). En la actualidad hay casi 150 millones de usuarios de Internet en Europa Occidental, una cifra que se cree que aumentará a 246 millones en el 2005(3). En 2005, se cree que Europa Occidental tendrá un 68% de participación en el uso de Internet sin cable con unos 170 millones de usuarios. Esta es una cuestión importante, ya que las empresas están sufriendo una grave exposición a la falta de seguridad por la implantación de redes de áreas locales sin cable (WLANs - Wireless Local Area Networks); debido especialmente a que no se han instalado las medidas de seguridad apropiadas.

---

2.- "Los usuarios de Internet pasarán el billón en 2005". ETForecasts, 6 de febrero de 2002.

3.- Fuente eT Forecasts 2001

Los usuarios públicos, con frecuencia, se consideran la parte más vulnerable para la intrusión, debido a la falta de concienciación de la seguridad de la información y de la utilización de estas herramientas que les protejan. Son pues especialmente vulnerables a la violación de la intimidad, al fraude de robo de identidad etc. Existe una preocupación generalizada de que el aumento de las "always-on connections" (siempre conectado a la red) supone una amenaza muy seria para aquellos que no instalan unas medidas de seguridad razonables y que ésto es un blanco fácil para la posible intrusión.

### ¿QUIÉNES SON LOS INFRACTORES?

Dentro de la Unión Europea, muchos de los Estados miembro tienen grupos de piratería informática operando dentro del país. Una de las amenazas de estos grupos es que frecuentemente para ser aceptados dentro del grupo y para escalar puestos dentro de la organización deben demostrar que son competentes con hechos. Por lo tanto, la cultura en sí misma aumenta la piratería y la sofisticación de las técnicas utilizadas.

148

Ha habido una proliferación de las herramientas de ataque, sobre todo las de naturaleza automatizada. Esto se ha avivado gracias a la cultura de la piratería. Un pequeño número de personas o incluso una sola persona puede paralizar a una organización. Pasando a través de múltiples servidores, utilizando cuentas pirateadas o copiadas y borrando ficheros de control, de esta forma eliminando cualquier prueba de sus actividades un buen pirata puede evitar ser detenido.

El pirateo en general está siendo cada vez más organizado, ya sea a través de grupos de presión, grupos de interés especial, con un elemento delictivo o grupos con algo que demostrar. El próximo paso es la actividad delictiva organizada.

Es probable que los delincuentes profesionales estén cada vez más implicados con las oportunidades que ofrecen las distintas formas del cibercrimen. A través de estructuras más flexibles, fluidas, más sencillas, la delincuencia organizada posee una mayor capacidad para conocer y acceder a nuevos mercados según van surgiendo.

Los niveles de sofisticación demostrados por la delincuencia organizada para las operaciones de negocios pueden verse a través de la contratación de especialistas que lleven a cabo varios aspectos de las actividades delictivas. La selección de especialistas de Tecnología de la Información y de la Comunicación es probablemente una progresión natural de la delincuencia organizada.



El comercio a través de la red es también muy lucrativo y es probable que la delincuencia organizada dirija sus pasos hacia él. Las oportunidades de fraude y de conseguir un coche procedente del blanqueo de dinero son una posibilidad demasiado lucrativa para ser ignorada por la delincuencia organizada.

La delincuencia organizada ha escogido su país de residencia como refugio seguro desde el cual pueden orquestrar sus diferentes actividades transnacionales.

La misma naturaleza de Internet se adapta perfectamente a este modelo permitiendo operaciones desde países que pueden ser considerados refugios seguros en los que las jurisdicciones pueden llegar a impedir una investigación. Los grupos de delincuencia organizada cuentan con países a través de los cuales pueden llevar a cabo sus chanchullos sin tener que preocuparse de ser interrumpidos por la Policía.

### **¿CUÁLES SON LOS DESAFÍOS PARA LA POLICÍA?**

Uno de los mayores desafíos a los que se enfrenta la Policía al luchar contra los casos de delincuencia internacional de alta tecnología es su capacidad para llevar a cabo investigaciones coordinadas eficazmente en diferentes jurisdicciones y sistemas legales.

149

Internet ofrece la posibilidad de una comunicación instantánea. Además de esto, está el hecho de que tal comunicación puede protegerse fácilmente a través del despliegue de medios sencillos. Tales técnicas pueden incluir el uso de un software anónimo; simulación de direcciones de protocolos de Internet(4) y de otra información; el uso de servidores por poderes para navegar por Internet; codificación, etc. Algunos de estos métodos requieren un grado de habilidad técnica bastante alto, sin embargo muchos no y con poca idea e investigación pueden ser fácilmente utilizados.

Es probable que los países que quieren atraer los negocios puedan adoptar sin problema actitudes relajadas hacia negocios allí, creando de esta manera refugios seguros para los datos mejor que vérselas con las jurisdicciones de paraísos fiscales y secretos bancarios.

Las Naciones Unidas concluyeron en un informe realizado en 2001 que "muy pocos países tienen legislaciones adecuadas que contemplen el ciberdelito y que de esta forma proporcionan refugios seguros para los ciberdelincuentes". Las legislaciones arcaicas y desfasadas se citaron como

---

4.- La dirección del protocolo de Internet es una serie de números que indican una dirección única del ordenador que está conectado con la Red (Internet en este caso).



un serio problema y se recalcó que en algunos países existían mecanismos de observancia muy débiles. Al avance en esta área ha contribuido el Consejo de Europa con el Convenio sobre el Ciberdelito que proporciona un modelo para los países que se basa en la definición de delito.

El convenio del Consejo de Europa requiere la tipificación de pirateo informático y los mecanismos del pirateo, la interceptación ilegal de datos, la interferencia en los sistemas informáticos, el fraude, la falsificación y la pornografía on line. También requiere el que se preste atención a la cooperación internacional de la Policía a través de la asignación de poder de las autoridades nacionales para llevar a cabo búsquedas informáticas y la incautación de datos. Cuarenta y tres países se han suscrito a este convenio, aunque no se sabe el nivel de desarrollo al que han llegado los países firmantes en cuanto a la aplicación del convenio.

Internet proporciona a los delincuentes un alcance mundial, anónimo, comunicación segura e instantánea, acceso a conocimientos, más objetivos y una gran cantidad de oportunidades para el delito y facilita las actividades existentes.

150

Los Cuerpos de Seguridad se enfrentan a enormes retos al tratar los desafíos que plantean el uso de nuevos métodos de comunicación; la mayor sofisticación de la tecnología y de los delincuentes. Se dejan rastros electrónicos, sin embargo estos pueden conducir y, de hecho, conducen a un callejón sin salida; también puede ser manipulado para dificultar las investigaciones. Estos nuevos desafíos suponen un cambio en las técnicas de investigación de los Cuerpos de Seguridad.

El sentido común del delincuente de la Tecnología de la Información y de la Comunicación le lleva a realizar acciones sencillas para reducir las oportunidades de ser detectado. Esto está sucediendo y puede ser que imposibilite a la Policía seguir la pista e identificar a los delincuentes. Existen muchos caminos para proporcionar formas de anonimato y disminuir las posibilidades de ser detectado. Algunos de estos métodos requieren un alto grado de habilidad técnica, sin embargo muchos no la tienen y con poca idea y realizando pocas investigaciones pueden fácilmente hacer uso de ellos.

La información digital es una fuente adicional de pruebas que puede bien ser un lugar del delito en sí mismo o una extensión de lugares de delitos en un mundo físico. El tamaño cada vez mayor de los sistemas de almacenamiento de datos desafía a la capacidad de la Policía para examinar los medios interceptados. Como tarea básica de las Unidades de Delincuencia Informática de los Estados miembro, se encuentra el análisis forense de los instrumentos de almacenamiento de datos, éste es un aspecto muy importante. Va a haber una mayor demanda de aptitudes forenses de la Poli-

cía. El tema se complica por el enorme volumen de datos que las pruebas pueden contener en mayor medida desde el 11 de septiembre así como el volumen de datos recogidos.

La Policía no se enfrenta únicamente al desafío de que el tamaño del almacenamiento de datos aumente, sino también con la variedad de dispositivos para su almacenamiento. Todos los nuevos dispositivos de comunicación y de medios de comunicación pueden contener datos relativos al comportamiento criminal y están siendo ampliados. La integración de los aparatos de comunicación móviles e Internet aumentarán sin duda la oportunidad delictiva e incluso representarán mayores desafíos para la Policía.

Se requieren nuevas estrategias para responder a la pérdida cada vez mayor de los recursos de la Policía en este campo, que inicialmente son a menudo menos de los necesarios

Los delincuentes están utilizando cada vez más la tecnología en sus actividades y, por lo tanto, es difícil descubrir un delito sobre todo los que son de una naturaleza organizada, que no cuentan con un elemento de alta tecnología. ¿Qué significa esto para la Policía? Significa que va a haber una mayor demanda de investigación sobre ciberdelitos y una mayor capacidad forense de los Cuerpos de Seguridad. Esto es respecto a recursos en el sentido de personal formado en toda la Policía a nivel local, regional y nacional. El “hardware” y el “software” que normalmente está actualizado según los avances tecnológicos. La investigación y el desarrollo para mantener al día los nuevos desafíos en este campo. El futuro es digital y la Policía necesita posicionarse proactivamente para poder responder a los desafíos que esto conlleva.

151

## LA AMENAZA

### **¿Es el ciberdelito una amenaza?**

Es una amenaza grave actualmente y continuará creciendo con los avances de las Tecnologías de la Información y de la Comunicación en todas las facetas de la vida, con el aumento de los objetivos y las oportunidades. El hecho de que los impactos del ciberdelito en todos los aspectos de la criminalidad y de que a menudo el delito del mundo real tiene un componente de alta tecnología (y viceversa) sólo conlleva una mayor confirmación de la gravedad de la amenaza.

### **¿Cómo se presenta el futuro?**

Debido al hecho de que no todo se denuncia y de que en algunos casos los delitos no son detectados se crea una situación en la que no se



conoce el auténtico ámbito y naturaleza, ésta es en sí la amenaza. Parte de la amenaza procede de fuera de la UE; es una amenaza global y sin fronteras. Por lo tanto, puede ser difícil o imposible el seguir la pista. La disponibilidad de la información y la propiedad intelectual es alta a través de Internet. Las instituciones financieras operan cada vez más on line y el comercio en Internet está aumentando, esto conlleva la vulnerabilidad de la información asociada. Por ejemplo, los datos de las tarjetas de crédito, proporcionándose de esta forma una mayor oportunidad para el delito. La centralización de las funciones clave dentro de las empresas y el gobierno que son impuestas por la informática está aumentando y así surge la vulnerabilidad de la información y de confianza en la informática y las redes que pueden ser objetivos y desorganizarse. La presión para crear sistemas abiertos y muy funcionales vía Internet en combinación con la falta de concienciación sobre la seguridad de la información han proporcionado una situación apropiada para la explotación.

### **Se espera que se incremente la amenaza en el futuro**

Todas las formas de delito verán aumentar las oportunidades con la expansión de las comunicaciones, las finanzas y el comercio. La amenaza está creciendo a la vez que Internet y el modus operandi está cambiando a la vez que los avances técnicos.

152

Internet se convertirá en parte natural de las operaciones comerciales de los grupos de Delincuencia Organizada. El punto anterior implica la selección de expertos en Tecnologías de la Información y de la Comunicación tanto por parte de los grupos de delincuencia organizada a gran escala como de otras empresas criminales a más bajo nivel para facilitar las operaciones en este campo.

### **¿Puede la Policía responder a la amenaza?**

Debido a la falta de un conocimiento estratégico y político del cibercrimen la amenaza no puede definirse completamente, y por lo tanto no se puede responder.

Se desconoce el alcance y la naturaleza del fenómeno, y éste está cambiando y renovándose continuamente, debido al entorno existen problemas inherentes con la creación de nuevas políticas de actuación muy efectivas de la Policía. La actuación policial reactiva ha rebasado los recursos en muchos países, debido sobre todo al volumen de trabajo forense y se requieren estrategias policiales llevadas a cabo con información proactiva efectiva.

La asignación de los recursos a la Policía para abordar el delito informático de alta tecnología dentro de los Estados miembro y de



Europol no está en la misma línea que la naturaleza horizontal del delito, por ejemplo hacer frente a todos los tipos de delito. La inversión no parece estar en la misma onda que la visión de e-Europe de la Comisión Europea que es conseguir los siguientes puntos más o menos en 2005:

- La visión de e-Europe es conseguir modernos servicios on-line (e-gobierno, e-votaciones, e-aprendizaje, e-servicios de salud).
- Un entorno e-comercio dinámico y próspero.
- Extender la disponibilidad del acceso a la banda ancha a precios competitivos.
- Una infraestructura de la información segura.

Todo lo anteriormente mencionado se conseguirá al compartir la información cada vez más y el procesamiento cooperativo entre los sistemas de "back-office" y la interoperabilidad entre varias infraestructuras y sistemas tanto a nivel nacional como internacional.

Se pone un gran énfasis en fomentar la confianza entre el e-usuario y el e-consumidor. El objetivo de acelerar la entrada de la UE en la era de información se traduce como el que los Estados miembro tienen Internet como tema de máxima importancia en su agenda, billones de euros invertidos en la visión de e-Europe.

Es esta visión y este dinero invertido lo que no parece estar en la línea con la inversión de recursos por parte de la Policía en el campo de las investigaciones de delitos de alta tecnología.

La e-Europe 2005 es parte del impulso para los negocios, el gobierno y el público para acoger la nueva tecnología. Esto traerá confianza y reforzará la economía. Sin embargo, algunas partes de esta visión pueden ser debilitadas por la actividad criminal y es por esta razón por la que se deberían dedicar a adoptar más recursos para asegurar que esto no ocurra.

La inversión de la Policía tiene que ser reconsiderada a nivel político y de altos cargos.

Sería verdad decir que las Unidades de Delincuencia Informática están sobrecargadas de trabajo y que no están en situación de rechazar solicitudes o trabajo, esto significa que la priorización ocupa un lugar muy importante en la práctica. Por lo tanto, el trabajo atrasado es algo habitual, lo cual tiene repercusiones posteriores en otras áreas de trabajo de la Policía en las que los casos y las investigaciones pueden estar en suspenso debido a los recursos limitados en el contexto del análisis forense.

## CONCLUSIONES Y RECOMENDACIONES

Existe la necesidad de un mayor entendimiento entre aquellos que deben tomar decisiones sobre el que el delito de alta tecnología es horizontal y tiene repercusiones en todos los tipos de delito. Este hecho debe ser representado a través de una asignación adecuada de los recursos, ya que las demandas de los expertos de la Policía en este área son grandes y aumentarán.

La falta de conocimiento y concienciación entre los que deben tomar decisiones ha sido resaltada como el problema central para muchas de la Unidades de Delincuencia Informática de los Estados miembro según la investigación de Europol, de esta forma incide en la asignación de recursos. Europol ha desarrollado un curso sobre la concienciación de los altos mandos que pronto será ofrecido a los Estados miembro que tiene como finalidad centrarse en la búsqueda de remedio a través de la educación.

154

Todas las clases sociales han tenido acceso a las Tecnologías de la Información y la Comunicación e Internet es de alcance global. Con el crecimiento de las Tecnologías de la Información y Comunicación y el interés por Internet estamos viendo un acompañamiento para el delito. Es difícil obtener una perspectiva adecuada de la extensión del delito en la época del trabajo en la red por las razones obvias que las empresas se niegan a denunciar y la ausencia de descubrimiento en algunos casos. Sin embargo, el ámbito y la complejidad del delito en esta área aumentará. Europol ha dado el primer paso elaborando un análisis estratégico que es la fundación y creación de un bloque para el posterior trabajo de inteligencia. Debe saberse que un ciclo estratégico de inteligencia es obligatorio para un conocimiento adecuado de este fenómeno.

Las Tecnologías de la Comunicación y la Información facilitan todas las formas de criminalidad a través de la comunicación. Internet proporciona a los delincuentes un alcance mundial, anonimato, comunicación segura al instante, acceso a los conocimientos, mayores objetivos y abundancia de oportunidades para el delito y para facilitar las actividades existentes.

La retención de datos es considerada a menudo como un aspecto polémico que puede y de hecho impide las investigaciones de la Policía. Es un área en la que el consenso dentro de la Unión Europea contribuiría en gran medida a los resultados, ya que todos los implicados se pueden beneficiar de un punto de vista común y los resultados que esto puede traer. Europol ha dado algunos pasos en esta dirección para apoyar y coordinar los diferentes esfuerzos ya adoptados en los Estados miembro.



Están bien consideradas las iniciativas llevadas a cabo por el Comisión de la Unión Europea para presentar una política global en el contexto de la Comunicación de la Comisión "Creando una sociedad de información más segura por medio de la mejora de la seguridad de las infraestructuras de la información y de la lucha contra el delito informático". En especial, las propuestas legales anunciadas en la "Ciber Crime Communication" prepararán el camino para una infraestructura legal armonizada y una mayor cooperación. Sin embargo, también debería prestarse atención a las medidas no legales para mejorar la cooperación entre las diversas unidades especializadas en los Estados miembro. Europol debería jugar un papel crucial y todos sabemos que el ciberdelito es un problema internacional que requiere una respuesta internacional. La cooperación y la coordinación son imprescindibles para abordar con éxito este problema. Europol se ha posicionado para jugar este papel dentro de la Unión Europea a través del trabajo llevado a cabo por medio del desarrollo de su Centro para el Delito de Alta Tecnología.

Las principales funciones de este centro reflejan las funciones tradicionales de Europol como por ejemplo:

- Intercambio de información rápido incluyendo los datos personales a través de los Oficiales de Enlace de Europol (Red ELO) y el intercambio "on-line" de información a través de Virtual Private Network (VPN) con un portal de Europol.

155

Europol está en contacto con muchos compañeros de los Estados miembros, intercambio información sobre investigaciones incluyendo datos de personal a través de una red de reconocido prestigio de Oficiales de Enlace de Europol y también recopilando los requerimientos de los Estados miembros para futuras actividades. Una de las principales necesidades es compartir experiencias y directrices de buenas prácticas. La consideración de la investigación del delito cibernético es viable por medio del aprendizaje a través de la práctica; la teoría es un complemento para ello. Por esta razón, la necesidad de tener un forum on line para el intercambio de información técnica por encima de la Red ELO ha sido una cuestión muchas veces planteada por los expertos de los Estados miembros y existe actualmente un VPN que conecta a algunos de los Grupos de Delincuencia Informática de los Estados miembro.

- Apoyo de inteligencia con evaluaciones de riesgo y amenaza y análisis de operaciones.

Europol lleva a cabo unos Informes de Situación y Evaluaciones de Amenazas sobre diversas áreas del delito vinculadas al delito grave y organizado. El Centro trata de proporcionar a los investigadores



una inteligencia integrada y estructurada desde todas las fuentes y partes implicadas. Esto puede conllevar por un lado la descripción de las redes y organizaciones criminales, el rol criminal y las actividades propias, la identificación de vínculos entre los criminales y sus actos, pero por otro lado también el análisis de lagunas de información. Para la recopilación de inteligencia importante, las actividades on line deben ser incluidas en el proceso de análisis. Basándose en los perfiles de interés individuales, los datos recogidos de Internet pueden contribuir en gran medida a los Ficheros de Trabajo Analítico de Europol (por ejemplo, en el área de terrorismo, el interés por las páginas web del mundo árabe o por ejemplo en las redes establecidas por Grupos específicos de Crimen Organizado como por ejemplo las bandas de moteros de los Ángeles del Infierno).

– Coordinación de investigaciones transfronterizas.

La prioridad de Europol es apoyar las investigaciones transfronterizas en curso y coordinar los esfuerzos de los Estados miembro. Las expectativas son altas respecto a este tipo de apoyo de Europol y complementadas con el análisis operativo directo ya ha sido probado que tiene éxito en las investigaciones internacionales.

156

– Investigación, desarrollo y formación

El Centro reúne de forma activa información sobre los nuevos desarrollos tecnológicos, las herramientas y los productos disponibles para las aplicaciones de los Cuerpos de Seguridad e intenta dirigir los proyectos de investigación externa. Se podría observar, por ejemplo, filtrando la información de Internet para extraer modelos de comportamiento criminal con el objetivo último de predecir actos criminales. El apoyo con éxito a la formación para temas de pornografía infantil e investigaciones relacionadas con Internet continuará. Además, una visión estructurada proporcionada por Europol sobre los cursos de formación existentes en los Estados miembros apoyará una cooperación más cercana. Aparte de ofrecer seminarios para la concienciación para altos cargos, la propuesta de proporcionar cursos de acreditación en el futuro también seguirá en la agenda de Europol.

Como ya se mencionó anteriormente, el futuro es digital y los Cuerpos de Seguridad necesitan posicionarse de forma proactiva para poder responder a los desafíos que esto conlleva.

La asignación de recursos de la Policía para abordar el crimen informático de alta tecnología dentro de los Estados miembro y Europol no está en la misma línea con la naturaleza horizontal del delito por ejemplo el

impacto en todos los tipos de delito. La inversión no parece corresponderse con la visión de la e-Europa.

Sería cierto manifestar que los Grupos de Delincuencia Informática están sobresaturados de trabajo y no están en posición de rechazar las propuestas de trabajo, de esta forma el significado de que la priorización juega una parte muy importante de la práctica del trabajo. Por lo tanto, cantidades enormes de trabajo atrasado son algo habitual, lo cual tiene impactos posteriores en otras áreas de trabajo de los Cuerpos de Seguridad en las que los casos y las investigaciones pueden esperar debido a los recursos restringidos en el ámbito del análisis forense.

La inversión de los Cuerpos de Seguridad debe ser revalorada a nivel político y de altos mandos.

# LOS PUNTOS CRÍTICOS TECNOLÓGICOS EN LOS SECTORES PRODUCTIVOS

**Bernardino Cortijo Fernández**  
**Vicepresidente de Seguridad de Terra**

## INTRODUCCIÓN

Cuando pretendemos valorar la situación real de una empresa, pública o privada, tenemos que considerar un factor importante, entre los muchos necesarios: los riesgos y vulnerabilidades, y qué se está haciendo para evitarlos. Vamos a tratar algunas ideas en relación con los denominados puntos críticos, en el apartado de las tecnologías asociadas a la Seguridad de la Información.

159

Veamos la repercusión de la problemática que estamos analizando en el entorno empresarial y en relación con la seguridad tecnológica, valorando y comentando experiencias que en el campo de la nueva seguridad puede suponer para esta parte de la población que busca, como todas las empresas, obtener beneficios, mover sus activos, y en definitiva jugar su papel en la sociedad.

En los momentos en los que estamos hay una serie de problemáticas que van surgiendo, pero tenemos medios para que la respuesta de prevención, de disminución de riesgos sea lo más rápida posible y con la menor eficacia por parte de los que intentan atentar contra el buen funcionamiento de las estructuras y de las organizaciones.

Hay muchos sistemas para reducir los riesgos. Pero primero vamos a ver cuáles son, en qué situación nos encontramos en las empresas, especialmente las relacionadas con la tecnología.

Es fundamental tener una concienciación de lo que es la seguridad, pero desde el punto de vista de los usuarios, de los intermediarios, desde la empresa privada a la pública. Cuando digo concienciación me refiero a



nivel de seguridad física, a nivel de seguridad integral donde todo el mundo está muy mentalizado y a nivel de la seguridad de la información, de seguridad lógica de datos. Tenemos la sensación de que utilizamos la informática para todo, pero no conocemos la situación a nivel de riesgo.

Lo primero que hay que hacer es concienciarse de que la situación es similar tanto en el mundo virtual como en el no virtual y que los puntos críticos que existen en todas las empresas se pueden determinar, identificando los riesgos y las contramedidas que deben establecerse para que su incidencia sea mínima y no afecte a la actividad diaria.

## PUNTOS CRÍTICOS

### Redes corporativas y redes exteriores

Por un lado hay que señalar las vulnerabilidades que nos afectan. Tenemos que distinguir el "hardware" - servidores, máquinas...- de los datos, de las bases, de las propias redes. Hay que diferenciar los distintos canales y programar y prever las vulnerabilidades ya que el ciberterrorismo y el cibercrimen, están ya afectándonos.

160 Actualmente las empresas en el mundo disponen de redes abiertas, redes que están expuestas, con puntos críticos de seguridad, que tienen que tomar medidas tanto a nivel interno como externo. Por mucho que nos blindemos de cara al exterior, internamente tenemos una serie de riesgos que también hay que proteger, aunque no tuviéramos salida al exterior, mucho más cuando damos entrada, como es lógico, a Internet y a otras redes.

Por tanto hay que diferenciar las vulnerabilidades y los puntos críticos que vamos a tener en el interior de nuestra empresa, en nuestro entorno de trabajo, ya sean usuarios, datos, bases de datos o nuestros propios servidores, de lo que es el exterior. Exterior que está bastante condicionado por la actividad empresarial, dado que hay un comercio exterior que puede ser comercio on line, tiendas virtuales, relaciones con proveedores, elaboración de productos que transportamos a través de la red, etc... En resumen, se trata de proteger el interior en alguna parte claramente definida.

Vamos a tratar los accesos. ¿Quién puede acceder a los ordenadores, a los datos? Por supuesto estamos hablando de la red interna y ahí hay muchas vulnerabilidades muy importantes en la empresa.

Tenemos que recordar, por ejemplo, los puntos de atención al cliente que hoy tienen todas las grandes empresas, centros de atención a los que se puede acceder para requerir un servicio, para solucionar un problema, una queja... Estos centros tienen acceso y conexión a los datos internos de la empresa, aún no estamos en la parte exterior, aquí no hay venta, ni comercialización estamos en la parte interna de accesos internos; pero hay una serie de elementos críticos, de puntos críticos, y pueden ser aprove-

chados por una persona directamente, con un medio electrónico o no, enviándolo por correo, recogiendo en un disco pequeño (USB) o apuntándolo en un papel puede sacar una información. Por eso es muy importante establecer soluciones globales, fijando normas de seguridad y procedimientos especiales de actuación, que nos permitan reducir riesgos, y no sólo tecnológicos.

Esto es un riesgo, sin duda, pero además están los riesgos propiamente de acceso, de vulneración de acceso, que los veremos mucho más exagerados en la red exterior al entrar en Internet hay muchas posibilidades de que haya terceros que quieran entrar y lo puedan conseguir.

Refiriéndonos al control de los datos, hablamos de virus, de troyanos, de distintos elementos que pueden introducirse externa o internamente en nuestras bases de datos y sacar información o comerciar con ella.

Y luego está todo el elemento relacionado con los propios servidores. Cuando hablamos de servidores estamos hablando de servidores corporativos, separando un poco los servidores de datos que en muchos casos están en sitios diferentes y en centros diferentes. Estén físicamente en el mismo sitio o fuera de él tenemos que realizar una protección de todos estos elementos. Así, por ejemplo, deberán existir segmentos estancos de red, según criticidad de datos y procesos, en los servidores de datos corporativos, medidas contra incendio o acceso en los servidores corporativos, pero también con una configuración segura de la plataforma en su conjunto, en la que podemos contar con una monitorización de actividades "anormales".

161

En algunas empresas puede coincidir la red externa física con la red interna, pero a efectos lógicos son redes distintas.

El uso de las redes externas nos plantea algún problema novedoso que estamos detectando, como son las redes inalámbricas. Hicimos un chequeo en algunas ciudades de EE.UU. y teníamos hasta un 70% a 80% de cobertura inalámbrica, que se podían vulnerar con facilidad. En los próximos años se van a convertir en un problema, son unas redes que, en los momentos actuales, no tienen los mismos elementos de protección que las redes a través de cables.

Se están colocando elementos de red en puntos donde la protección no está totalmente salvada con cortafuegos o elementos externos, entre otras cosas porque a veces ni se utilizan elementos de protección que existen en las máquinas o software.

En Estados Unidos ya se han detectado problemas con las agendas electrónicas, con las que se puede acceder a la red y lanzar comandos de sistema. En España aún no se han detectado problemas significativos en este sentido.

Además tendríamos el uso de las redes a través de Internet, a través



de las tarjetas de red que tengamos colocadas y ya veremos algunas complicaciones que existen con ellas, igual que con el sistema de acceso interno, hay distintas formas de proteger el acceso externo a las redes internas y a las redes de comercio o de información y hay sistemas más seguros y menos seguros.

Lo que si es cierto es que el mercado quiere seguridad, pero también comodidad. El usuario quiere agilidad, se niega a tener que teclear cuatro veces una password o que le pidan datos al entrar en una página web. Esto hay que valorarlo y conseguir el mayor nivel de seguridad pero sin entorpecer las entradas.

### IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

Respecto al riesgo, no se encuentra únicamente ante un virus o un hacker que entra y saca unos números de tarjetas. El riesgo se identifica con tres parámetros: los activos, las vulnerabilidades y las amenazas.

Los activos te permiten diferenciar qué vulnerabilidad está tocando y qué dimensión de la vulnerabilidad tienes, diferenciando las amenazas que puedes prevenir en cada uno de los casos.

162

Por ejemplo, al introducir los datos de nuestra tarjeta de crédito para comprar algo a través de Internet tenemos un riesgo. La protección frente a éste no debe ir dirigida exclusivamente a proteger la comunicación entre el cliente que mete los datos y el servidor del banco que los recoge, sino que debe ser integral desde un punto de vista normativo, porque si no en algún punto se puede escapar la seguridad, desde un punto de vista tecnológico y desde un punto de vista organizativo. Por tanto hay que contemplar los tres parámetros. Así este riesgo será mínimo, incluso menor que cualquier actuación en el mundo no virtual (como pagar en un restaurante o gasolinera).

Para poder afrontar este tipo de vulnerabilidad hay que realizar un análisis de riesgos.

Ahora están proliferando las herramientas de análisis de riesgos más o menos inteligentes. Pretende que las vulnerabilidades que se vayan detectando no estén en manos de individuos, ni de bases de datos donde se pueda acceder, sino que estén automatizadas, lo que eran antiguamente los sistemas de inteligencia artificial pero que por su alto coste están en un periodo de retroceso, salvo proyectos especiales.

Pero para el análisis de riesgos además hay herramientas informáticas que nos lo facilitan más dinámicamente. Actualmente estas herramientas son escasas en el mercado mundial porque son programas complejos y con su utilización podemos tomar dos tipos de medidas importantes: las procedimentales y las tecnológicas.

Hay herramientas que son el reflejo del día a día que permiten ir



identificando los riesgos y para ello hay que conocer las vulnerabilidades, identificarlas, se van colocando, las tenemos diferenciadas y posteriormente incluso se puede hacer un análisis de riesgos más detallado. En cada una de esas casillas se van colocando la acción posterior que tomemos. La actividad de Gestión de riesgos se explota en varias actividades clave, incluyendo las de análisis de riesgos. De realizarse de forma continua, se consigue reducir los niveles de riesgo residual a un nivel aceptable.

Algunas acciones son automáticas. Por ejemplo en un sistema operativo de una compañía se ha detectado una vulnerabilidad, ella misma la ha descubierto y hay que subsanar esa deficiencia. Alguna de esas cosas se pueden hacer de forma automática y otras requieren de un mensaje de alarma para que lo puedan resolver los técnicos.

## MEDIDAS PREVENTIVAS

Por tanto para las medidas preventivas siempre hay que considerar los activos, las vulnerabilidades y las amenazas, pero se hace de forma progresiva, buscando solución a cada uno de los problemas que pudiera surgir:

- Protegiendo el activo o facilitando su recuperación ante una incidencia.
- Reduciendo la posibilidad de que una amenaza pueda actuar contra los activos.
- Reduciendo la exposición de la organización a ciertas amenazas.

163

Siempre se busca un conjunto equilibrado de controles de naturaleza organizativa y procedimental, todo lo relacionado con las seguridades lógica y física, las medidas de cumplimiento legal y las campañas de concienciación e imagen.

Por lo tanto, primero habría que hacer una clasificación sencilla organizativa y procedimental, culminando en las políticas de seguridad que todo el mundo debe conocer en cada uno de sus aspectos. Segundo, partamos de lo que es la seguridad lógica como tal, relacionada con los elementos de seguridad lógica que existen en el mercado, valorar lo que hay y coordinarlo con lo que tenemos y buscar la mejor solución. Si no protegemos la CPD, de poco servirá protegerse a través de la red.

En tercer lugar, todo lo que es el cumplimiento legal. En España la L.O.P.D, nos obliga a adoptar medidas de seguridad importantes, al igual que la L.S.S.I. Además es importante observar la normativa de otros países ya que puede interesar acercarse a sus directrices. Véase el Convenio del Cibercrimen, adoptado en el marco del Consejo de Europa, a falta de ratificación.

Por otro lado, tenemos que concienciarnos, todos, no sólo el usuario, sino las empresas, y la propia Administración en la necesidad de inver-

tir en seguridad.

La imagen es muy importante, hay muchos temas que van contra la seguridad pero que realmente son sólo un problema de imagen, no existe un problema técnico. Por ejemplo, si alguien entra en la página web de una empresa comercial y la cambia, aunque no haya accedido a los datos, ni provocado problemas en el comercio on line, y el usuario lo llega a conocer no confiará y no se atreverá a introducir los datos de su tarjeta de crédito.

Dentro del entorno de la seguridad probablemente todas las empresas dispongan de medidas de seguridad de todo tipo. El desafío está en encontrar la adecuada combinación entre ellas.

A nivel preventivo se suelen tomar más medidas, medidas físicas ya que todo el mundo tiene una cerradura, un sistema sofisticado de seguridad, un sistema de mantenimiento de energía o antiincendios.

A nivel lógico tenemos los cortafuegos, los elementos de seguridad de redes, software específico para nuestras subredes, antivirus o controles de acceso.

A nivel humano repartimos el trabajo de la seguridad y lo delegamos en distintos elementos que no son siempre informáticos: procedimientos laborales, supervisión, formación técnica o concienciación en seguridad, entre otros.

164

A nivel de detección una vez encontrado el incidente, una vez localizado el hacker vamos a buscar qué ha pasado. A ese nivel se toman menos medidas y eso dificulta la labor policial. Si existe un hecho de este tipo y no se almacena información de lo que ha ocurrido, malamente se podrá llevar a cabo una investigación posterior. A nivel empresarial el problema es el mismo, al resolver un problema interno de empleado o uno externo de intrusión, ni lo vamos a poder hacer solos, ni con la Policía, si no tenemos una serie de elementos de detección preparados para realizar esa tarea. Esto también incluye medidas físicas o lógicas.

A nivel organizativo pasa exactamente lo mismo, tenemos lo tradicional pero estamos pensando en relacionar estos elementos y relacionarlos con un análisis de riesgo. Esta es la fase que más avanza.

## POLICÍA Y LA SEGURIDAD EN LAS REDES

Por todo ello se crean, en todos los países, las unidades especializadas relacionadas con este campo tan especializado de la delincuencia. Así nos encontramos con la Unidad Central contra los Delitos en Tecnologías de la Información, creada en 2000, actualmente Brigada de Delitos Tecnológicos, dentro del Cuerpo Nacional de Policía. Es necesario disponer de ellas y estar al unísono y facilitarles la información necesaria para que pue-



dan trabajar: almacenamiento de datos, posibilidad de recuperación, ...

Las legislaciones se van uniformando en lo relacionado con las nuevas tecnologías. En el entorno del cibercrimen tenemos varias legislaciones, algún foro de trabajo a nivel mundial, incluso en coordinación con las empresas, como hace Europol. En el fondo lo que se pretende es que todos dispongamos de una legislación similar. Poco a poco se va consiguiendo, pero aún nos encontramos con paradojas singulares. Al respecto hay ejemplos de todo tipo.

## **CASUÍSTICA, CIBERCRIMEN Y CIBERTERRORISMO**

Esto no es ciencia ficción, ya no es algo que está empezando, está muy avanzado. Tenemos la pornografía infantil, lo relacionado con la propiedad intelectual, con las tiendas virtuales, operaciones cada vez más sofisticadas. Ahora nos encontramos con actitudes intermedias desde las propias organizaciones que van realizando operaciones con el nombre de la empresa y luego nos hacen el timo virtual, luego no pagan la gran operación y lo hacen en otra provincia distinta después de haberse ganado la confianza de una empresa grande, o de gran volumen de ventas, por ejemplo informáticas y me refiero a estos productos por ser más caros y ser más fácil sacar un rendimiento rápido.

Para poner un ejemplo de la realidad con la que nos encontramos cada día, vamos a ver la equiparación entre el mundo virtual y el mundo físico. Cada delito en el mundo virtual tiene su equivalente en el mundo físico.

165

Las entradas forzadas, las entradas en establecimientos. ¿Cómo se hacen a través de la web? Tenemos todo tipo de entradas.

Según un resumen estadístico del FBI con otras entidades de recuperación de datos, en el que conjugan las denuncias efectuadas con la recogida de datos en las empresas o a los usuarios de forma anónima; parece que el porcentaje de intrusión ha aumentado un 65%. Este porcentaje ha recibido un ataque en sus empresas y en sus ordenadores.

A mi me ha llamado la atención que las intrusiones exteriores hayan aumentado un 28%, cuando han disminuido las interiores.

Hasta ahora se ha dicho que el riesgo mas grande de los hackers estaba en casa, en algún momento alguien pasaba datos, tenía una puerta falsa, estaba vendiéndose al exterior, etc... Un 70% de las intrusiones estaban dentro.

Parece ser que las intrusiones desde fuera, lo que implica vulneración de equipo, vulneración de software y un mayor conocimiento por parte del intruso.

Yo no sé si esto es totalmente fiable ya que la recogida de datos es a nivel empresarial y quizá la empresa no quiera reconocer que un



empleado suyo ha sido desleal.

En otro orden de cosas es curioso lo que llamamos el graffiti. En algunas ocasiones supone un problema grave y en otras es simplemente una cuestión de imagen.

Hay alguna web que nos permite ver on line, en cada momento los ataques que se están efectuando, incluso pinchando en cada uno de ellos para que veamos que está así.

Esta web está mantenida por hackers intermedios que reciben información de los atacantes. Una cosa curiosa de los atacantes es que les gusta que se conozca su acción, salvo que quieran atacar a alguien.

Algunas web han sido vulneradas muchísimas veces. Cada pocos minutos hay ataques exitosos de modificación de sitios web.

Ahora vamos a comentar algunos casos de cambio a nivel de imagen.

La página de la Cámara de Comercio Argentina, donde el hacker dejó su huella. Algunos llegan a dejar hasta la foto. En otros casos los mensajes que dejan pueden revelar motivaciones u objetivos sociales o políticos en su actividad. Tenemos el grupo Hacking for Satan, ilegal pero controlado en EE.UU.

166

Un caso muy llamativo fue el de la compañía Air Tran que vendía a través de Internet a precios muy económicos. Un avión tuvo un fallo y se quemó al despegar, murieron varias personas. Alguien sustituyó la página y puso un avión en llamas y el mensaje en inglés "entonces matamos a unos cuantos ¿y qué?". Nadie durante un tiempo quiso viajar en sus aviones y estuvo a punto de quebrar. Incluso las empresas o entidades dedicadas exclusivamente a la seguridad a veces son hackeadas.

Otro tema fundamental es el relacionado con los virus.

Hoy, a nivel de empresa, los más problemáticos son los virus de red, que además van evolucionando, me refiero a los que no llegan al equipo, por lo que los antivirus hay que colocarlos en los servidores de red. Se detectan tarde lo que complica mucho la solución. Estos transmiten virus a los ordenadores que estén dentro de la red.

Importante también son los ataques de negación de servicios, llamados ataques DOS. Es el talón de Aquiles de Internet. Consiste en recibir un montón de peticiones desde distintos sitios, la máquina contesta y los peticionarios no aceptan la respuesta. De esa forma se bloquean los recursos del sistema de los ordenadores, se colapsan, ya que están previstos para recibir una petición y contestar y aunque estén preparados para miles y millones de usuarios, realizando el ataque desde muchos miles de puntos a la vez se puede bloquear el sistema. Estos ataques evolucionan para no ser detectados. Esto puede provocar problemas muy graves en las empresas. Si

van orientados a un proveedor de Internet o de comunicación puede paralizar los servicios, no sólo de esa empresa, sino de miles de personas y otras empresas.

En el mundo financiero se conocen pocos casos, pero los hay. Recordaremos el caso de Vladimir, un individuo relacionado con la mafia rusa, que hizo cientos de transacciones, se le “cogió” en una de ellas contra Citibank por 12 millones de dólares. No se recuperaron más que 400.000 y se le puso una multa de 240.000 y tres años de prisión. Se calcula que se pudo apoderar de muchísimo más en otras actuaciones.

Otro caso es el de algunos alumnos de los últimos cursos de la Universidad de California que cogieron los números de la tarjetas de crédito de un servidor de la Universidad para a través de la Wester Union hacer transferencia a cuentas virtuales en otros países donde no podían ser detectadas. No se recuperó casi nada.

También fue curioso el hecho ocurrido en una empresa “ICQ” (empresas que dentro del entorno de los chats o mesanger actúan como intermediarios financieros, tienen un apodo o NIK y con él trabajan) donde un hacker se apoderó de su password y vulneró el NIK, por lo que no podían trabajar. Parece que el hacker pidió 100 \$, se le dio y hoy trabaja para ellos.

Hace unos años se detectaron 5,6 millones de tarjetas de crédito, de las que se habían sacado los datos de los clientes. Las compañías de crédito tuvieron que establecer contacto con los clientes, darles unas nuevas y en su caso devolverles el dinero, si se habían utilizado las tarjetas.

Se están buscando soluciones on line, no sólo para transacciones económicas, sino de datos, como son los sellos de seguridad.

Un problema cada vez más preocupante es el de la piratería, tanto a nivel de música como de películas, se piratea incluso las películas que están en cartelera. España lidera la piratería a nivel de software. Esto está relacionado con algo que aquí se está subsanando y es la venta de los ordenadores con software, como en otros países donde el índice de piratería es menor.

Otro problema que cada día prolifera más es el de la usurpación de identidad. Por ejemplo el spoofing de correo electrónico, donde se sustituye el origen del correo.

A nivel de empresa es muy importante la utilización lícita de los medios de Internet a través de los medios de la empresa.

Una empresa tuvo que indemnizar a un empleado despedido por ver “porno”, por Internet, en su horario de trabajo con los medios de la empresa, porque no disponía de una advertencia que le avisara de que no podía utilizar Internet más que para los fines de la empresa.



Se dice que un 9% de los internautas, la mayor parte mujeres, están enganchados a Internet.

En Internet además de los millones de servidores que hay por todo el mundo existen otros que se llaman NODOS que centralizan la información y la gestión otros ordenadores y luego hay alrededor de 13 servidores grandes en todo el mundo. Estos 13 servidores gestionan en primera instancia las direcciones a las que se quiere acceder en Internet. Esto quiere decir que si hackeamos alguno de estos equipos el rendimiento de la red mundial baja. Si machacamos 2 ó 3 o la mitad de la red bajaría muchísimo más y si machacásemos todos no habría Internet, aunque funcionaran las redes.

Estos puntos son puntos de ataque constante de los hackers.

## ACCIONES

¿Qué se puede hacer contra los ataques de ciberterrorismo?

168 - Establecer una política corporativa de seguridad que conciencie a la organización y marcar objetivos de seguridad. En este sentido hay que considerar la necesidad de recurrir a estándares o quasi estándares, como la ISO 17799 o la BS 7799, las "best practises", Magerit, cramm, ... y en todo caso a una metodología para adaptar a las necesidades de cada organización. Posteriormente la elaboración de unos procedimientos de detalle técnicos y legales que afecten a cada sistema informático, a cada proceso de recuperación o plan de contingencia.

- Actualizar inmediatamente los sistemas de la organización, en cuanto que surgen parches de seguridad de los proveedores.

- Considerar dispositivos o sistemas específicos de protección si la amenaza lo justifica. Esto justifica las inversiones en sistemas integrales de seguridad o en medidas de carácter lógico y de protección de la información, pero basados en las políticas de seguridad ya establecidas.

- Mantenerse al día en las alertas de seguridad en la red.

- Tener en cuenta las directrices gubernamentales sobre el ciberterrorismo.

- Colaboración con las Fuerzas y Cuerpos de Seguridad.

- Cooperación internacional



## ALGUNAS CONCLUSIONES

Para concluir quiero transmitirles que:

- El control de riesgos es fundamental en la empresa y da valor a una compañía.
- Hay un sinnúmero de puntos vulnerables y críticos en los sistemas telemáticos de las empresas, sobre todo cuando éstos están conectados a Internet.
- Consecuentemente es necesario emplear periódicamente algún proceso de identificación, análisis y valoración de riesgos tecnológicos.
- El nivel de exposición a los riesgos da lugar a una selección equilibrada de medidas preventivas, para reducir los riesgos a un nivel aceptable.
- El ciberterrorismo y el cibercrimen son hechos. Organismos públicos y, sobre todo, la Policía tienen un papel importante en conseguir un nivel de confianza generalizada en las transacciones por Internet.

## TERCER PANEL

PROTECCIÓN, DETECCIÓN Y RESPUESTA



# **INICIATIVAS PÚBLICAS DEL MINISTERIO DE CIENCIA Y TECNOLOGÍA EN EL ÁMBITO DE LA SEGURIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES**

**Salvador Luis Soriano Maldonado  
Subdirector General de Servicios de la Sociedad  
de la Información  
Ministerio de Ciencia y Tecnología**

173

## **INTRODUCCIÓN**

El término “Sociedad de la Información” del que tanto venimos hablando en los últimos tiempos puede entenderse como una incorporación creciente de las tecnologías de la información y de las comunicaciones a todos los ámbitos económicos y sociales, transformando de manera sensible las pautas de comportamiento de los ciudadanos en la esfera laboral y personal.

Si analizamos el desarrollo de la Sociedad de la Información merece prestar una particular atención a la rápida extensión de Internet a lo largo de toda la geografía mundial. Esta extensión se ha basado en los reducidos costes de acceso y la amplia disponibilidad y capilaridad de la infraestructura que proporciona la tradicional red telefónica instalada a lo largo de décadas.

Internet ha creado una conectividad mundial que pone en contacto millones de redes y cientos de millones de ordenadores individuales con una ingente cantidad de información disponible y un elevado número de interlocutores potenciales.

Nos encontramos actualmente en una situación en la que las tecnologías de la información y las comunicaciones se han incorporado en



nuestros hábitos rápidamente por su elevada utilidad y se han convertido en elementos insustituibles para la vida cotidiana de ciudadanos y empresas.

Resulta fácil imaginar las dificultades para llevar a cabo nuestras actividades diarias si, por ejemplo, fallara la operativa de las entidades bancarias o se borrara o se introdujeran errores en la información de nuestras cuentas, desapareciera o perdiera su integridad la información contenida en los ordenadores de las empresas sobre su contabilidad, su gestión de aprovisionamiento y almacenamiento, sus datos sobre los clientes o los datos de facturación, fallaran los sistemas informáticos de emisión o reserva de billetes aéreos, ferrocarriles o dejaran de funcionar los mercados bursátiles nacionales o extranjeros, etc.

Esto pone en evidencia que existe una cada vez mayor dependencia de la economía de los países, y de la vida de los ciudadanos en general, del correcto funcionamiento de las redes de comunicación que transmiten la información y de los sistemas que la gestionan, constituyéndose éstos en elementos críticos cuyo funcionamiento debe ser convenientemente protegido.

Esta seguridad de la información y las comunicaciones es un nuevo reto que debe ser afrontado en esta Sociedad de la Información que se configura. En tanto esta seguridad no se perciba como claramente reforzada y se regenere suficiente confianza en los ciudadanos existirá un obstáculo importante para el mayor desarrollo del comercio electrónico y para las relaciones telemáticas en general.

Para reforzar la seguridad de la información y las comunicaciones deben ser considerados el cumplimiento de los siguientes principios:

- **Confidencialidad**, entendida como el aseguramiento de que la información es accesible sólo para aquellas personas autorizadas.

- **Disponibilidad**, entendida como la garantía de que los usuarios autorizados tienen acceso a la información cuando lo requieran.

- **Integridad**, entendida como la garantía de que la información y sus métodos de proceso son exactos y completos y de que no ha sido modificada indebidamente.

- **Autenticidad de origen en las comunicaciones**, entendida como la garantía en las comunicaciones de que el origen de una información está identificado de manera única e inequívoca.

Desde el Ministerio de Ciencia y Tecnología se están desarrollando diferentes líneas de actuación en relación con la seguridad de la información y las comunicaciones, que a continuación se describen de manera general y resumida.

## ACTIVIDADES DEL MINISTERIO DE CIENCIA Y TECNOLOGÍA EN EL ÁMBITO DE LA SEGURIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES

### Actividades de ámbito internacional.

En primer lugar, puede destacarse la participación del Ministerio de Ciencia y Tecnología en foros internacionales relacionados con la definición de políticas públicas europeas sobre seguridad, en particular, en la Unión Europea. Así, se ha participado en la elaboración de las Resoluciones del Consejo de 28 de enero de 2002, relativa a un enfoque común y a acciones específicas en materia de seguridad de las redes y de la información y en la de 18 de febrero de 2003 sobre un enfoque europeo orientado hacia una cultura de seguridad de las redes y de la información.

Por otra parte, hay que recordar que en el Plan de acción eEurope 2005, aprobado durante la Presidencia Española de la Unión Europea, se contempla el objetivo de que antes de finalizar 2005, debe construirse una «cultura de la seguridad» en el diseño e implementación de productos de información y comunicaciones. Para ello, se debe fomentar la aplicación de unas buenas prácticas en la gestión de la seguridad de la información y sensibilizar a todos los usuarios sobre los riesgos asociados a la falta de seguridad de las redes y la información.

175

Además, existen otros foros internacionales en los que el Ministerio participa y que son particularmente activos en materia de seguridad de la información y las comunicaciones como el “working Party on Information Security and Privacy” de la OCDE.

En el ámbito internacional resulta asimismo destacable la participación desde el Ministerio de Ciencia y Tecnología en la definición de una Agencia Europea de seguridad que sirva de centro de conocimiento, asesoramiento y divulgación de las herramientas de seguridad a disposición de ciudadanos y empresas europeas. En relación con esta Agencia Europea, se ha presentado ya un borrador de Reglamento para su creación por parte la Comisión Europea.

### Programas nacionales de promoción de la seguridad de la información y las comunicaciones.

En lo que se refiere al ámbito nacional, y desde un punto de vista operativo, el Ente Público Empresarial RED.ES, gestiona el denominado Centro de Alerta Temprana sobre virus y seguridad informática, donde se ofrece asesoramiento en materia de seguridad.

Otras de las funciones del Ministerio de Ciencia y Tecnología es apoyar desde sus programas de ayudas económicas los proyectos innovadores relacionados con la seguridad de la información. Así, en el programa PROFIT se ha establecido una acción estratégica específica para la seguri-



dad y confianza de las tecnologías de la información, donde tiene cabida numerosos proyectos de innovación en esta área.

También se han financiado la realización de estudios sobre el estado de la seguridad de la información en España, en particular, el pasado 7 de mayo se presentó el elaborado por la Asociación ASIMELEC "Estudio sobre el estado actual de la seguridad de los sistemas de la información en las empresas españolas de acuerdo con la Norma ISO-IEC 17799", del que se extraerán conclusiones para hacer más efectivas las medidas de apoyo a la mejora de la seguridad de la información en nuestro país. Este estudio está disponible de manera gratuita en la dirección de Internet [www.asimelec.es](http://www.asimelec.es).

Asimismo, se ha dado apoyo, en el marco del programa Arte/Pyme a la iniciativa de la citada Asociación ASIMELEC de realizar un ciclo de 21 Jornadas sobre seguridad y confianza en la red a lo largo de toda la geografía española.

176 La campaña de 21 Jornadas que actualmente está aún en fase de desarrollo se dirigirá en particular a las pequeñas y medianas empresas, que es el tejido empresarial con mayores dificultades de disponibilidad económica y de recursos humanos para abordar estas áreas de cierta complejidad técnica. En las Jornadas se han incluido aplicaciones concretas de seguridad basadas en herramientas de firma electrónica, presentadas por prestadores de servicios de certificación relevantes como la Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda, Camerfirma o IPSCA, constituyéndose en un complemento práctico adecuado a la actual modificación del marco regulatorio de sobre firma electrónica en España.

### **El marco regulatorio para la firma electrónica**

Una de las facetas más importantes del Ministerio de Ciencia y Tecnología en lo que se refiere a la seguridad de la información y las comunicaciones es el impulso de la regulación en el área de la firma electrónica.

La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

La nueva regulación de la firma electrónica, elaborada en estrecha colaboración con los Ministerios de Justicia, Economía, Interior y Administraciones Públicas, tiene el objetivo de fomentar la rápida incorporación de las tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones Públicas. De este modo, se potencia el crecimiento y la competitividad de la economía española, mediante el establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet.



El nuevo proyecto de Ley de Firma Electrónica surge del compromiso asumido de tramitar el anterior Real Decreto-Ley 14/1999 como Proyecto de Ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. En esta nueva redacción, que ya ha sido aprobada por el Gobierno y se ha remitido al Parlamento, se han incorporado las modificaciones que aconseja la experiencia acumulada desde la entrada en vigor del Real Decreto-Ley en el año 1999, tanto en nuestro país como en el ámbito internacional.

En cualquier caso, la regulación española debe establecerse con total respeto a los principios establecidos en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

Antes de analizar el marco regulatorio de la firma electrónica, resulta de interés destacar que la situación actual de utilización de la firma electrónica en España, aunque incipiente, es relativamente satisfactoria teniendo en cuenta el desarrollo de esta herramienta de seguridad en los países de nuestro entorno.

Así, puede destacarse que los servicios telemáticos de la Agencia Tributaria española, basados en la utilización de la firma electrónica, se han convertido en una referencia europea e incluso mundial de las relaciones telemáticas en el ámbito tributario entre los ciudadanos y las Administraciones. Durante la campaña de la declaración del impuesto de la renta de las personas físicas del ejercicio 2.002, se han presentado 1.718.000 declaraciones telemáticas, registrándose elevados crecimientos en los tres últimos años.

177

### **Principales elementos del marco regulatorio de la firma electrónica**

En lo que se refiere al marco regulatorio de la firma electrónica, los aspectos básicos recogidos en el mismo pueden resumirse de manera general y sin carácter exhaustivo en los siguientes:

Las entidades que se constituyen en la base de los sistemas de firma electrónica son los prestadores de servicios de certificación, que expiden los denominados certificados electrónicos, que son documentos electrónicos que relacionan las herramientas (claves) de firma electrónica con la identidad del firmante, siendo los garantes y responsables del establecimiento del vínculo entre el entorno físico y el telemático.

Por ello, el correcto comportamiento y diligencia de estas entidades es de especial relevancia en la generación de confianza en los sistemas de firma electrónica y a estos prestadores se dedica una gran parte de la regulación: obligaciones, responsabilidades, infracciones y sanciones.

El Proyecto de Ley define una clase particular de certificados electrónicos denominados certificados reconocidos. Estos certificados deben

ser expedidos cumpliendo requisitos especiales en lo que se refiere a: su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica desarrollada por el prestador de servicios de certificación.

El Proyecto de Ley establece un conjunto de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad, teniendo en cuenta y equilibrando las responsabilidades de estas entidades con los deberes de diligencia de los firmantes y terceros destinatarios de documentos firmados electrónicamente.

Los prestadores de servicios de certificación deben efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada Declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

178

Los certificados reconocidos constituyen la base de la llamada firma electrónica reconocida que se define, siguiendo las pautas establecidas en la Directiva 1999/93/CE, como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. A la firma electrónica reconocida se le otorga en la Ley, respecto de los datos consignados en forma electrónica, una equivalencia funcional con la firma manuscrita.

El Proyecto de Ley contiene las garantías técnicas que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar con su utilización una firma electrónica reconocida equivalente a una firma manuscrita.

Finalmente, puede destacarse que se establece un régimen de supervisión y control por parte del Ministerio de Ciencia y Tecnología, y un régimen de infracciones y sanciones aplicables a los prestadores de servicios de certificación.

### **Modificaciones más relevantes incluidas en el Proyecto de Ley de firma electrónica**

Con el objetivo de dinamizar el mercado de la prestación de servicios de certificación, el nuevo Proyecto de Ley incorpora novedades en relación con el Real Decreto-Ley 14/1999 sobre firma electrónica, exponiéndose a continuación las principales.

Se elimina el Registro de prestadores de servicios de certificación, al objeto de dar mayor dinamismo a la prestación de servicios de certifica-



ción. En contrapartida, se establece un mecanismo de recopilación y publicación de información para dar a conocer la oferta de servicios disponibles en el mercado que efectuará el Ministerio de Ciencia y Tecnología, eliminándose las infracciones por la falta de comunicación de esta información por parte de los prestadores.

Se incluye la regulación del Documento Nacional de Identidad Electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos.

El Proyecto de Ley se limita a fijar el marco normativo básico del DNI electrónico, poniendo de manifiesto sus dos notas más características - acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

El DNI electrónico permitirá instaurar una cultura de uso de la firma electrónica entre los ciudadanos que favorecerá el desarrollo de nuevas aplicaciones, potenciando al sector en su conjunto.

Se introduce el régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático. Se va así más allá del Real Decreto-Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas jurídicas.

En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Se desarrollan las relaciones de representación que pueden subyacer en el empleo de la firma electrónica. La representación está ampliamente generalizada en el tráfico económico, de ahí la conveniencia de dotar de seguridad jurídica la imputación a la esfera jurídica del representado las declaraciones que se cursan por el representante a través de la firma electrónica.

Se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, para el cumplimiento de sus obligaciones tributarias, en los términos que establezca el Ministerio de Hacienda.



Se desarrollan con mayor detalle los medios para la identificación de los solicitantes de certificados reconocidos (al ser esta identificación una de las claves de la confianza telemática) que deben ser utilizados por los prestadores de servicios, dado que esta identificación que permite enlazar el mundo físico y telemático es fundamental en la generación de confianza. Asimismo, este mayor detalle no implica inflexibilidad, sino que se introducen ciertos criterios de flexibilidad para la renovación de certificados, para la obtención de nuevos certificados basándose en otros certificados similares de los que ya disponga el firmante o para el expedición de certificados basándose en una relación preexistente.

Se clarifica y suaviza la obligación de constitución de una garantía económica para hacerla más asequible por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Se incluye la definición de firma electrónica reconocida, que es la firma electrónica que se equipara funcionalmente a la firma manuscrita, realizándose esta figura y clarificándose que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación de firma.

180

Se limita la responsabilidad de los prestadores de servicios de certificación, al considerar también los necesarios supuestos relacionados con la diligencia y custodia que corresponden a los firmantes y destinatarios de firmas electrónicas.

Los prestadores de servicios de certificación quedan eximidos de responsabilidad por la inexactitud de los datos contenidos en un certificado si éstos le han sido acreditados mediante documento público. En caso de que dichos datos deban figurar inscritos en un Registro Público, el prestador deberá comprobarlos en el momento inmediato anterior a la expedición del certificado, pudiendo emplear para ello medios telemáticos

Se prevé que los prestadores de servicios de certificación puedan, con el objetivo de mejorar la confianza en sus servicios, establecer de manera voluntaria mecanismos de coordinación con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos. Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los Registros a los prestadores de servicios de certificación de las variaciones registrales posteriores.

Por otra parte, el Proyecto de Ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones

legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la Directiva. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación.

El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público.

Se mantiene un esquema de mayor control únicamente para la certificación de dispositivos seguros de creación de firma electrónica, con una supervisión del Ministerio de Ciencia y Tecnología.

Por otra parte, siguiendo la pauta marcada por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

Dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que el Proyecto de Ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología, señalando que este Departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

## **HACIA UNA CULTURA DE SEGURIDAD TECNOLÓGICA**

**Adrián Moure Lledó**

**Presidente de la Comisión para la Seguridad y la Confianza  
de las Tecnologías de la Información (ASIMILEC)**

Mi ponencia está dirigida a explicar la situación actual de la seguridad como consecuencia directa de la entrada en la vida de las empresas y usuarios de las tecnologías de la información. El mayor problema al que nos enfrentamos y al que se enfrentan las organizaciones cuando hablan de la seguridad, es que suelen circunscribirla a las áreas informáticas, a las áreas de sistemas, a la sala de servidores y se suele pensar que es sólo allí donde están los problemas de seguridad y por tanto los conflictos que hay que solventar.

183

Las empresas actualmente dependen de los sistemas informáticos, y por tanto, estamos planteando un escenario donde si el sistema informático se para, el negocio de las compañías, también se para.

No es que alguien lea un correo o que entre en nuestra Web. El problema es que si alguien consigue parar nuestro sistema, se pierden horas de trabajo, se pierden clientes, se pierde dinero, se pierde prestigio, se pierde imagen, en definitiva la empresa en su totalidad se colapsa.

Además, tenemos una legislación y una normativa internacional que obliga a adoptar una serie de medidas de seguridad. La LOPD, que es el caso más claro que tenemos, nos obliga a establecer una serie de medidas que están muy bien descritas en el reglamento y que tienen un régimen sancionador.

Entonces no estamos ante una cuestión voluntaria, que una empresa decida: "Quiero dar un mejor servicio a mi cliente", simplemente estamos ante una cuestión legal, ante una ley que tiene un régimen sancionador y que puede suponer que acabemos con una multa muy importante.



A todos estos problemas se ha intentado durante todos estos años ponerle solución mediante productos tecnológicos, mediante soluciones técnicas. “Tengo un problema de virus, pongo un antivirus. Tengo un ataque, pongo un firewall. Tengo un problema de apagones, pongo un sistema de alimentación ininterrumpida”. Pero todo esto siempre lo hacemos “a toro pasado”, una vez tenido el incidente. Las soluciones, no son algo que simplemente compro, monto y milagrosamente han resuelto el problema.

La cuestión dista bastante de eso, la seguridad es realmente un proceso, no es producto, es algo que tenemos que gestionar, mantener y planificar.

Estamos ante una situación en la que los incidentes se duplican cada año. Supongo que Vds. están hartos de oír hablar de este tipo de situaciones o de leerlo en los periódicos. Pero las estadísticas demuestran la evidencia. A pesar del incremento de las nuevas tecnologías, con nuevos productos maravillosos que nos prometen resolver los problemas y la desaparición absoluta de incidentes. Aún con todo esto, a pesar de ello, se siguen duplicando los incidentes cada año.

184

Tenemos cada día entre dos y cinco nuevas vulnerabilidades. Entendemos como vulnerabilidad el descubrimiento de un fallo, de una puerta atrás en una aplicación que estamos utilizando, en un navegador, una vía de entrada, una debilidad que hay en el sistema informático que tenemos implantado. Y permite a un tercero poner en marcha una agresión, levantar información, tirar un sistema. Pues cada día aparecen entre dos y cinco nuevas vulnerabilidades.

Esto quiere decir que nuestra infraestructura que hoy es perfectamente segura, esta perfectamente configurada y no tiene ni el más mínimo problema, con las nuevas vulnerabilidades puede quedar rebasada. Eso hace que las soluciones tecnológicas no sean suficientes por si mismas, que haya que gestionarlas, haya que mantenerlas, haya que revisarlas. Normalmente cuando se habla de seguridad siempre se piensa en confidencialidad, siempre se piensa en proteger un documento. “Esta información que tengo es confidencial y por lo tanto tengo que mejorar mi seguridad para protegerla”.

La seguridad se basa en realidad en cuatro ejes estratégicos, y así se entiende a todos los niveles. Tanto en las normativas internacionales como en las directivas que ha elaborado el Ministerio de Administraciones Públicas.

Por un lado está la autenticación, tenemos que verificar que quien está intentando acceder, es quien dice ser, eso en el mundo físico es muy sencillo, alguien llega y dice: “Buenos días, soy José Ángel Suárez Pérez”. “¿Me deja su DNI?” “Sí aquí lo tiene”. Miras el DNI, le miras la cara y ya le has autenticado. Pero en Internet eso no es tan sencillo, yo me conecto a través de un ordenador, me piden un login y una palabra clave, yo las meto y el ordenador asume que es cierto lo que afirmo. Pero en la realidad puedo ser yo, o alguien que me haya visto meter las claves, las haya memorizado y que vaya a trabajar a partir de ese momento en mi nombre.

Por lo tanto, autenticar al que pretende entrar, es un problema de seguridad y bastante serio.

El siguiente problema que tenemos es el de la confidencialidad, supone garantizar, que sólo puede acceder a la información quien tenga derecho a ello.

El otro parámetro es la integridad, que garantiza que la información a la que se pretende acceder es completa, es exacta, no ha sido modificada.

El otro eje es la disponibilidad, estar seguros que cuando accedamos a los sistemas, la información esté disponible permanentemente.

Con lo cual realmente estamos ante una cadena de elementos, donde muchos puntos tienen que controlarse y si no se vigilan todos, pues por algún sitio se acabará rompiendo.

Siempre que se habla de seguridad se piensa en los ataques externos, un hacker, un virus o un ataque a través de la ADSL.

Tenemos que entender que cuando hablamos de seguridad no sólo estamos hablando de que alguien externo entre, estamos hablando también de que la información esté disponible siempre y de que sea exacta. Por eso, uno de los principales problemas que tenemos es nuestro personal, gente que internamente ataca los sistemas, quiere cotillear los ficheros o están enfadados. Me contaban el caso de un responsable de sistemas que le despidieron y cogió el cubo del agua de la fregona y lo volcó por encima del grupo de servidores, dejando todo absolutamente bloqueado. O sea que no estamos hablando necesariamente de ataques muy sofisticados, puede haber ataques verdaderamente de fuerza bruta.

Tenemos problemas de interrupción del suministro eléctrico, si se va la luz el sistema informático se cae, y no podemos seguir trabajando, no necesariamente tiene que ser un virus, algo tan trivial como que se vaya la luz, nos puede afectar gravemente. Tenemos accidentes, hay incendios, hay tuberías que se rompen, hay máquinas que se averían, todas estas cuestiones provocan que nuestro sistema informático se pare y por lo tanto tengamos incidentes de seguridad.

Por último tenemos errores de seguridad, los usuarios cometen errores, las personas cometemos errores en un momento determinado porque normalmente no tenemos una formación básica sobre el uso de los sistemas o sobre aspectos relacionados con la seguridad. Y aquí no me refiero a que sepan configurar un firewall, o integrar en las aplicaciones un sistema de cifrado asimétrico. Estamos hablando de aspectos más cotidianos, de aspectos más triviales. Si Vd. manda algo a imprimir algo, por supuesto que sea confidencial: el balance de la compañía, el plan estratégico, los salarios del año próximo, según le da al comando de imprimir váyase a la impresora y recoja el documento, porque como tenga una llamada y no lo recoja en ese momento, tarde o temprano esa información, terminará por quedarse en la impresora y alguien la acabará cogiendo.



Si Vd. va a mandar un correo electrónico con un fichero confidencial, si lo manda con un correo sin cifrar, es a todos los efectos, una postal. Una postal va abierta y por todos los sitios por donde pase, se puede leer. Pues con el correo electrónico pasa exactamente igual, por cualquier sitio por el que pase un correo en claro, las personas por las que pasa, pueden interceptar ese correo y pueden leerlo, no es confidencial. Y ese tipo de cosas generalmente los empleados no lo saben, bueno, ni los empleados ni la dirección. Por correo electrónico se envía todo y en claro, y nadie entiende que después haya información confidencial de la empresa por ahí.

Entonces una medida de seguridad tan sencilla como es proteger ese tipo de documentos cifrándolos no se toma y eso complicaría muchísimo a todas esas personas por las que va pasando la postal, así no pueden abrir ese documento. Bueno pues de ese tipo de formación y de información es de lo que estamos hablando y de ese tipo de errores es de los que estamos hablando. Esos son los tipos de errores que complican muchísimo la seguridad y que resolverlos es trivial, simplemente es tener una charla de concienciación, de formación.

186 Informations Security Magazine informa, que la principal fuente de problemas hoy, sigue siendo el "código malicioso", virus, troyanos, gusanos, etc., pero después vienen los usuarios autorizados y además, la dirección de la compañía. Entre los usuarios autorizados y la dirección de la compañía, causan más problemas a la seguridad que los virus. Y estos son datos reales. Con lo cual no sólo tenemos un problema tecnológico, hay una tecnología que es imprescindible, pero también tenemos un problema de gestión, de concienciación, de conocimiento y estamos hablando de acciones que son muy sencillas. Darle una charla de dos horas a las personas que trabajan con los sistemas informáticos no tiene un gran coste, y por tanto no supone un gran esfuerzo financiero para la empresa y mejora muchísimo todos los elementos de seguridad. En seguridad no da un gran resultado las medidas reactivas, el: "a toro pasado", tomar medidas después, no es una buena política. Es necesario tener un plan previamente, conocer los riesgos, cuáles son los problemas, cómo se pueden solventar y en consecuencia preparar ese plan para abordarlos.

¿Cuáles son los problemas con los que se encuentran las empresas en el día a día? Ya no hablo de cosas muy sofisticadas: hackers, crackers, ataques muy complejos. En las empresas en el día a día, nos llegan correos y enviamos correos con información confidencial, con troyanos, con chistes, con películas, con música y por supuesto, con virus.

Cuando los empleados navegan por Internet, por el simple hecho de estar entrando en determinadas páginas, puedes llenar los servidores de correos de virus. Podemos quedar registrados en sitios desde los que van a hacer envíos masivos de correos (spam), además de perder muchísimas horas de trabajo navegando para fines personales, buscando ofertas para salir de puente, leyendo periódicos.



La proliferación de la banda ancha, lo cual es una oportunidad fantástica para el mercado de la telecomunicaciones y el comercio electrónico, genera que las empresas que están contratando ADSL en muchos casos no son conscientes de los problemas de seguridad que conlleva, y que necesitan adoptar medidas. Se suele pensar que si tengo una Frame Relay a 2Mb y cuesta un millón de pesetas todos los meses, entonces hay que poner un firewall, tengo que gestionar la seguridad, etc., pero si pongo una ADSL, como me vale 5.000 pts. al mes, no merece la pena que haga nada. Pero al final, el riesgo es el mismo. Tienes una dirección fija, con una línea fija conectada a la Red por donde te pueden atacar, o sea, que "sí", tienes que adoptar unas medidas de seguridad por el hecho de haber montado una línea que ya no es un MODEM. Porque en general, estas líneas están levantadas habitualmente.

Muchos de los problemas que tenemos están relacionados con el personal, el personal en general no conoce los problemas de los que estamos hablando o dicho de otra manera, aunque los conozca, no es consciente del riesgo que para la organización eso supone.

Además está "el Imprescindible". El imprescindible es esa persona que cada vez que pide vacaciones todo el mundo se hecha a temblar, porque como se vaya, no hay nadie más que sepa hacer la copia de seguridad, si se va de boda y se cae el sistema no hay nadie más que sepa levantarlo, si se va de vacaciones, como se averíe otra vez el disco duro del servidor nos volvemos a quedar parados una semana, etc, etc,

187

Es vital que las organizaciones prevean el riesgo del imprescindible. Este tipo de problemas se resuelve documentando y generando una serie de procedimientos, si esa persona es la que sabe hacer el backup, que escriba un procedimiento de cómo se hace el backup, y alguien que sea medianamente espabilado y tenga unos ligeros conocimientos de informática, podrá coger el procedimiento y seguirlo, en caso de que sea necesario.

Los imprescindibles son un problema para las empresas. No sólo porque en un momento nos pueden poner entre la espada y la pared con una petición fulminante de aumento de sueldo o cualquier otra historia, sino por el hecho de que esa persona puede romperse una pierna exactamente igual que cualquiera y puede estar de baja tres meses y vamos a tener un problema serio con la seguridad.

Con todo esto ¿qué es lo que tenemos? Las empresas se plantean el problema de la seguridad y llegan a la conclusión de que hay que hacer algo, se posicionan ante un escenario de este tipo y dicen: "Bueno vamos a adoptar una solución tecnológica que nos resuelva todos los problema de una vez y así volvemos a dormir tranquilos".

Ponen un antivirus, compran un firewall, un servidor de validación, un router, compran incluso un sistema de detección de intrusos, en fin, montan todo un señor sistema de seguridad, que por supuesto está perfectamente configurado, perfectamente dimensionado. Y esta empresa hoy, es

perfectamente segura, impenetrable. Pero mañana una de esas cinco nuevas vulnerabilidades que van a aparecer, afectan a su firewall, a su router o al navegador y resulta que lo que hoy era absolutamente impenetrable, mañana es un queso gruyere.

Esto es uno de los problemas de la seguridad, la seguridad se rompe frecuentemente y cuando se rompe, lo hace de forma impredecible, o sea hay un tiempo el que no sabemos si el incidente de seguridad es trivial y la nueva vulnerabilidad no tiene mayores consecuencias o si estamos ante un nuevo Nimda, que se va a llevar por delante el 40% de los sistemas informáticos. En consecuencia hay un tiempo en el que se pasa del aburrimiento al pánico en cuestión de minutos, hasta que averiguamos que es lo que pasa, entonces ¿cuál es la cuestión?, decir: "No hago nada, porque haga lo que haga, no voy a estar nunca seguro".

La cuestión no es solamente comprar mucha tecnología, sino también elaborar procedimientos, pensar cada cuanto tiempo voy a revisarlos, cada cuanto tiempo tengo que mirar si hay nuevas vulnerabilidades, cada cuanto tiempo tengo que pasarles nuevos parches a los servidores, actualizarlos etc.

188 No es complicado, lo único que hay que hacer es dedicar un poquito de tiempo a mirar los correos, a revisar las listas de vulnerabilidades, ver si tenemos algún problema y periódicamente, una vez al mes, hacer un pequeño análisis para mirar si tenemos algún agujero nuevo. Realmente no estamos hablando de la necesidad de muchos recursos para hacer esto.

Entonces la desesperación nos lleva a buscar una quimera: la panacea. Esa pastilla maravillosa que la tomas y de repente adelgazas sin necesidad de hacer dieta, sin hacer ejercicio, sin hacer nada de nada. Y eso no existe. No hay un producto barato, fácil de instalar, sin mantenimiento, que resuelva todos los problemas de seguridad y que además no tengamos que aprender nada nuevo, ni tengamos que cambiar ningún hábito de trabajo. Les garantizo que no lo hay.

Entonces la solución generalmente es la contraria, ante cada problema nuevo, o un nuevo incidente de seguridad, nosotros adquirimos más tecnología.

Es necesario cambiar esa filosofía y pensar que además, es necesario gestionar, configurar, poner orden.

¿Dónde tenemos uno de los problemas más grande en seguridad?

Como veíamos antes, uno de los problemas más graves son los usuarios autorizados. Hoy en día, hay técnicas de seguridad que son plenamente seguras, se dice: computacionalmente seguras.

Un algoritmo de cifrado fuerte de 1024 bit es seguro, no hay forma de romperle, con lo cual se puede pensar: "Esto me permite garantizar la



confidencialidad, porque cifro un correo y nadie lo va a poder leer. Me permite garantizar la integridad, firmo un documento y si alguien lo modifica, yo lo voy a saber. Bueno, pues dos problemas de seguridad que me he quitado de en medio". ¿Pero cuál es realmente el problema? Que al final, todo esto lo tiene que manejar un usuario y ahí es donde la seguridad se rompe.

Por ejemplo, los usuarios no quieren usar password de calidad. "¿Cuál es tu password?": "Jose". "Pero es que Jose no es un buen password y sería mejor que lo hicieras más largo y además le añadieras una cifra": "Vale pues JoseJuan-3". "Sigue sin ser un buen password y además recuerda que debes cambiarlo todos los meses". "Vale, pues JoseJuan 4 y el mes que viene 5 y al otro 6".

Quieren poner un password que sea fácil de acordarse, que cada vez que accedan, no tengan que teclear mucho. Pero la facilidad para el hacker, es directamente proporcional a la simplicidad de nuestro password.

También generalmente nos enfrentamos a usuarios que normalmente no saben reaccionar ante problemas que ocurren de forma inesperada, cuando un ordenador empieza a ir mal, el usuario normalmente lo único que dice es: "ya está "esto" otra vez fallando". Pero el "ya está "esto" otra vez fallando", puede ser que haya un virus, o que alguien se ha introducido y está modificando el sistema, o simplemente que Windows una vez más ha vuelto a dar problemas. Pero alguien debe ser capaz de detectar eso, no se pretende que los empleados sepan adivinar donde está el fuego y como apagarlo, lo que si se pretende, por lo menos, es que sepan oler el humo, saber que huele a quemado y que avisen a alguien que sepa lo que hay que hacer.

Otro gran problema de la seguridad, es el de la ingeniería social, cuando se le preguntaba a uno de los mayores hacker norteamericano, cual era su método de ataque, que hacía para conseguir penetrar en los sistemas y vulnerar todos los niveles de seguridad de la CIA y del FBI, se le ofreció una reducción de condena, si revelaba sus técnicas que se suponían que eran análisis criptográficos o módulos supercomplejos, el individuo aceptó y les explicó que la metodología era buscar en las papeleras, en las bolsas de basura y sobre todo, preguntar. Era lo único que hacía.

Preguntando, conseguía prácticamente todo. Hay un principio en seguridad que dice: una cantidad determinada de información no confidencial, junta, puede constituirse en información confidencial. O sea, si yo no sé nada pero quiero entrar en una empresa, lo primero que hago es llamar y preguntar: "Buenos días, ¿me podría dar el correo electrónico del Director General, es que tengo que mandarle una invitación?" "Sí, apunte." "Perdón ¿me podría dar también el nombre y los apellidos?" "Sí, apunte". Un par de días después: "Buenos días, llamo de la empresa XXX tenemos aquí un regalo para D. Fulano de Tal y queríamos enviárselo a su casa, ¿me puede dar su domicilio?". Y te lo da. Al final vas juntando toda esa pequeña información que no es confidencial, pero al juntarla sí es muy impor-



tante y llamas otra vez y dices: "Hola, mira estoy aquí en la casa del Director General en tal domicilio, tal piso, he venido a configurarle el correo electrónico, pero el firewall me está parando el acceso, ¿le puedes decir al de sistemas que me lo abra un momento?". Y al final acaban por abrirlo.

Las empresas que se dedican a hacer auditorías y a hacer hackínicos usan mucho estas técnicas y consiguen verdaderas maravillas. Se consigue mucha información en este país, simplemente preguntando. La gente contesta con muy buena voluntad, para ayudar, y para ayudar nos da información que nos ayuda a entrar donde queramos.

Entonces como hemos ido comentando, tenemos muchos eslabones condicionando la seguridad, unos que son eminentemente tecnológicos, hay antivirus, hay cifrado, firewall, etc., y son absolutamente necesarios, pero tenemos también una serie de eslabones no tecnológicos y que son igual de imprescindibles.

Debe haber una política de seguridad, tiene que haber un plan, alguien tiene que haber hecho un análisis de riesgos para saber cuáles son nuestros potenciales problemas, dónde están, de qué tamaño son. Porque en función de lo grandes que sean, así tendremos que invertir en tecnología. Podemos comprar un firewall por 100.000 pts. o por 15 millones. O sea la horquilla es como cuando vamos a comprar un coche, puedo comprar un SEAT Ibiza o puedo comprar un Mercedes 500, pero lo primero es determinar cuáles son mis necesidades. Porque la cuestión, como decíamos antes, es que más tarde o más temprano, se nos va a romper la cadena, y siempre lo va a hacer por el eslabón más débil.

190

En el estudio que hicimos desde ASIMELEC para el Ministerio de Ciencia y Tecnología, pretendíamos averiguar cuál era la situación de las PYMES españolas con referencia a la seguridad. Hicimos un muestreo sobre las propias empresas que están en la Asociación, buscando conocer qué hacían, qué medidas tomaban, en qué punto estaban en inversión de seguridad. Entonces lo primero que preguntábamos era qué tecnologías tenían implantadas. Vimos que antivirus, prácticamente tenían todos y firewall algunos. El resto de las tecnologías prácticamente no se utilizaban.

Y por último lo que exploramos también, era qué aspectos cumplían relacionados con la seguridad que recomienda la norma internacional ISO17799. Vimos que prácticamente en todos los casos, las implantaciones estaban por debajo del 50%, pero en elementos como planes de continuidad de negocio, que son absolutamente críticos para la seguridad, la carencia era absoluta.

Un plan de continuidad de negocio, lo que nos permite es tomar decisiones previamente planificadas ante un incidente grave, mejor dicho, ante cualquier incidente. Hay que planificar los riesgos. Por ejemplo, saber hasta qué punto el correo es crítico para nosotros. Ante la rotura de una tubería que pasa por encima del CPD y se nos ha inundado, ¿qué debemos hacer?.

Necesariamente tiene que haber un plan previsto: qué es lo que se va hacer en esos casos. Y en las empresas que estuvimos entrevistando, ese nivel de implantación era muy escaso, se le daba más relevancia a aspectos más técnicos como control de acceso, gestión de comunicaciones y operaciones.

¿Cuál es el análisis de esto?. Que la seguridad antes se planteaba una visión exclusivamente técnica o tecnológica, y ahora hay plantear otro plano que es el legal, o sea tenemos que tener seguridad para estar dentro de la ley, aunque suene demasiado fuerte, pero es así. Además de una dimensión financiera, porque tenemos que tener seguridad para continuar operando, para continuar teniendo ingresos, para continuar teniendo la confianza de nuestros clientes, para seguir manteniendo nuestra imagen, nuestra credibilidad y por tanto seguir manteniendo nuestro estatus financiero.

¿Qué beneficios reporta gestionar la seguridad? Primero reduce las horas de inactividad, al haber menos caídas y esas caídas cuando las hay, ser más cortas. Al haber menos errores de uso, tener menos problemas. Todo esto, mejora la productividad de forma considerable.

También nos ayuda, el reducir las horas dedicadas a fines personales por nuestra gente, en España tenemos una dedicación media diaria de entre 30 y 90 minutos de cada uno de los empleados que acceden a Internet, para ver las fotos, leer chistes, responder a los correos que nos han mandado los amigos, navegar un rato por las Web, leer el Marca, leer otro periódico de noticias políticas, buscar ofertas de viajes para el siguiente puente. Han oído Vds. bien, se pierde en todas estas cosas entre 30 y 90 minutos cada día por persona.

Los problemas en seguridad son costes directos, cuanto entra un virus y se lleva por delante un montón de ficheros, que como es lógico, los teníamos en una copia de seguridad que nunca se había probado y cuando se prueba no funciona y al final se pierden los ficheros. O se rompe un disco duro. O nos entra un virus, en fin, cualquier incidente, supone un coste.

Está cuantificado que una pérdida de 20 Mg. en el departamento de MK, necesita para reconstruirse un coste aproximado de €25.000. Esa misma pérdida en el departamento de I+D o de Desarrollo tiene un coste de €85.000.

20 Mg. hoy en día se los lleva por delante cualquier nuevo virus, se pierden con cualquier incidente.

Una parte importante de los incidentes de seguridad se producen por errores, descuidos u osadías de los empleados. Por medio de la formación y las políticas de seguridad, estos incidentes se pueden reducir entre un 70% y un 95%.



Sobre todos estos temas nos dan recomendaciones desde distintos foros, uno de ellos es la OEDC, (Organización Europea para el Comercio y la Distribución). Nos indican que para resolver estos problemas de seguridad tenemos que empezar por abordar un plan de concienciación, ser conscientes de los problemas, de los riesgos y del papel que cada uno tiene dentro de la organización. Hay que distribuir responsabilidades, dejar muy claro quién es el responsable de cada cosa y por lo tanto, quién debe resolver cada problema. Que haya un cierto automatismo en responder a los incidentes, que cuando algo esté pasando, se dispongan de los medios, los recursos donde avisar para que alguien con capacidad real de solucionarlo se entere y en consecuencia adopte las medidas necesarias.

Por supuesto todo eso tiene que ser coherente con los principios de ética y de democracia. No podemos saltarnos a la torera los derechos a la privacidad, los derechos a la intimidad, ni podemos obviar ningún principio de un estado democrático. Todo lo que es seguridad debe estar basado en un análisis de riesgos, contenido dentro de un plan e incluido desde el propio momento del diseño de los sistemas. No es conveniente incluir la seguridad "a posteriori", cuando ya hemos implantado el CPD, cuando ya hemos desplegado el nuevo sistema, cuando ya hemos hecho la migración de los servidores, no es el mejor momento para ver lo que necesitamos en seguridad. Probablemente cueste el doble o el triple de lo que hubiera costado, si se hubiera hecho desde un principio.

192

Y por último todo eso hay que revisarlo, hay que disponer de un proceso escrito de mejora y revisión.

Y como conclusión recordarles otra vez que cada día las organizaciones dependen más de los sistemas informáticos, en algunos casos la dependencia es absoluta. Una entidad financiera hoy en día, si se le cae el sistema informático, se acabó, no hay forma de trabajar. Pero la seguridad basada en medidas técnicas no es suficiente, cada día tenemos nuevos riesgos que surgen, no se debe buscar quimeras o panaceas para resolver los problemas de seguridad, es un trabajo que se resuelve gestionando la seguridad cada día, tomando conciencia de que es un problema de todos y debemos lograr por tanto, la sensibilización de todos.

Hay que combinar las medidas técnicas con las de gestión. Hay que tener en cuenta el factor humano. Hay que formar al personal, hay que explicarles cual es su papel. No tenemos una situación ideal respecto a la inversión en seguridad en España a pesar de los esfuerzos en subvenciones que se están haciendo desde la Administración para fomentarla. Y es curioso, porque no hay ningún país en Europa que tenga las subvenciones que hay aquí, en ayudas en la adquisición de tecnología, estudios, etc.

Podemos gestionar la seguridad para reducir el gasto y tener un retorno de esa inversión, o sea, que lo que invertamos en seguridad lo podamos recuperar en productividad, en ahorro de costes y sobre todo en tranquilidad.



# **CENTROS DE ALERTA TEMPRANA, UN MODELO DE COLABORACIÓN**

**Antonio Amador Reyes**  
**Inspector del Cuerpo Nacional de Policía**  
**Jefe de Grupo de Seguridad Lógica de la Brigada**  
**de Investigación Tecnológica (BIT)**

## **INTRODUCCIÓN**

**193**

En los albores de Internet, cuando sólo se trataba de una red experimental de ordenadores que conectaban varias universidades estadounidenses, el Departamento de Defensa de EEUU fomentó la creación de una arquitectura de red segura para prevenir la interrupción del servicio en caso de una catástrofe nuclear que pudiera destruir algún servidor o eslabón de la red. Con esta finalidad se desarrolló el protocolo TCP/IP. Esta red estaba restringida a dar servicio a determinadas instituciones educativas y gubernamentales, y el principal elemento a proteger era la propia red.

Con el tiempo, esta red (ARPANET) fue introduciéndose en el ámbito público y empresarial constituyendo lo que hoy en día conocemos como Internet. La "red de redes" ha crecido tanto en los últimos años que se ha quedado pequeña y obsoleta, con lo que están apareciendo nuevos proyectos para su migración a la futura Internet2.

En un principio, el entorno de aplicación de la red estaba enfocado a usuarios "de confianza" (organismos estatales) y la seguridad consistía en asegurar que la red funcionase y los paquetes de datos tuvieran siempre una ruta hacia su destino final.

Internet no fue diseñada para soportar el uso actual que tiene y la aparición de todo tipo de usuarios ha puesto de manifiesto la fragilidad "a priori" de sus comunicaciones.

Por otro lado, el ritmo de desarrollo de las aplicaciones informáticas y sistemas operativos han generado fallos de programación que ponen al descubierto vulnerabilidades que pueden comprometer el correcto funcionamiento de un sistema.

En 1988 el número de servidores ascendió a unos 60.000. La aparición de un virus que afectó a una décima parte de los ordenadores puso de manifiesto la falta de seguridad en la Red y movió a la ARPA a formar el Computer Emergency Response Team (CERT), un equipo de reacción rápida que se encargaba de analizar las incidencias de la red.

En nuestro país, el Plan Nacional de Investigación y Desarrollo creó un programa para la Interconexión de los Recursos Informáticos (IRIS) de los centros de investigación. La Red IRIS fue el principal impulsor en temas de conexión de ordenadores y de formación de usuarios, gestionada por Fundesco (Fundación Telefónica).

Con el boom de Internet en España aparecieron varias iniciativas privadas donde se ofrecían servicios de alerta a los usuarios sobre la aparición de virus o vulnerabilidades que operaban paralelamente con el es-CERT o Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas gestionado por la Universidad Politécnica de Cataluña.

## ES-CERT

El esCERT-UPC tiene el mismo objetivo que los otros CERTs Europeos y del resto del mundo. El ámbito de actuación es todo el territorio del Estado Español, aunque la red académica dispone adicionalmente del Iris-CERT, donde hay una actuación conjunta.

El esCERT-UPC basa su actuación en el análisis, recomendación, formación y asistencia a emergencias. Estos servicios están personalizados y sujetos al secreto profesional. Mediante los análisis y las recomendaciones se realiza una auditoría de carácter periódico, mientras que la formación se lleva a cabo en forma de cursos-seminarios.

### ¿Qué son los avisos de los CERTs?

Los avisos de los CERTs dan información sobre como obtener un añadido o detalles de un problema conocido de seguridad. El CERT trabaja con los fabricantes para emitir un informe o un añadido para un problema determinado, y no lo hace público hasta que el informe o el añadido están disponibles. Un aviso del CERT también puede alertar sobre la continuidad de algunos ataques.

### ¿Dónde puedo encontrar los avisos de los CERTs?

Hay un grupo de las noticias donde el CERT publica sus avisos (comp.security.announce), y también una lista de distribución (cert-advisory). Una completa referencia de los avisos del CERT está disponible en

nuestro servidor (mirror de <ftp://info.cert.org>). También otros CERTs generan sus propios avisos, como el AUSCERT de Australia o el DFN-CERT de Alemania.

Se puede encontrar una completa referencia de avisos en nuestro servidor, de los cuales se realiza un mirror cada dos días.

### **¿Dónde puedo encontrar los parches descritos en los avisos de los CERTs?**

Normalmente el CERT no distribuye los añadidos. Algunas empresas distribuyen los códigos fuente, mientras que los otros distribuyen sólo los binarios.

### **¿Qué listas de distribución, grupos de noticias, u otras fuentes puedo consultar?**

- CERT advisory mailing list

Avisos del CERT. Para darse de alta enviar un mensaje a [cert-advisory-request@cert.org](mailto:cert-advisory-request@cert.org), poniendo en el cuerpo del mensaje SUBSCRIBE <tu email> . Puedes consultar los avisos en Avisos de Seguridad.

- CIAC-notes

Intercambio de información de herramientas y técnicas de seguridad. Para darse de alta enviar un mensaje a [ciac-listproc@l1nl.gov](mailto:ciac-listproc@l1nl.gov), poniendo en el cuerpo subscribe ciac-notes <tu nombre>. Para consulta a archivos <ftp://ciac.l1nl.gov/pub/ciac/notes/> o <http://ciac.l1nl.gov> si prefieres interface WWW.

- CIAC-bulletin

Intercambio de información de herramientas y técnicas de seguridad. Para darse de alta enviar un mensaje a [ciac-listproc@l1nl.gov](mailto:ciac-listproc@l1nl.gov), poniendo en el cuerpo subscribe ciac-bulletin <tu nombre>. Para consulta a archivos <ftp://ciac.l1nl.gov/pub/ciac/bulletin/> o <http://ciac.l1nl.gov> si prefieres interface WWW.

- Bugtraq mailing list

Discusión sobre agujeros de seguridad. Para darse de alta enviar un mensaje a [listserv@lists.securityfocus.com](mailto:listserv@lists.securityfocus.com), poniendo en el cuerpo subscribe bugtraq <tu nombre>. Puedes consultar los archivos a Security Focus, en el apartado Forums->Mailing Lists->Bugtraq. Existe una versión en castellano de la lista, llamada bugtraq-es, que funciona de manera similar.

**FUENTE:** <http://escert.upc.es>



## NATURALEZA DE LOS CENTROS DE ALERTA TEMPRANA

Históricamente, los centros de alerta temprana han sido constituido para prevenir determinadas catástrofes naturales como terremotos, fenómenos meteorológicos, etc. Su forma de actuación consiste en recoger información de campo, analizarla y prevenir un hipotético desastre antes de que éste ocurra.

La naturaleza de los centros de alerta temprana tecnológica o simplemente alerta tecnológica difiere un poco del modelo clásico. En este caso, la amenaza existe y se trata de avisar con tiempo a los administradores y usuarios para que tomen medidas al respecto. Un ejemplo claro son los virus informáticos; cuando un centro de alerta tecnológica detecta un nuevo virus, lo analiza y advierte de su existencia, difundiendo la protección correspondiente en algunos casos, con el fin de minimizar su propagación y los posibles daños que pueda ocasionar.

La cooperación de los distintos sectores sociales: administración pública, industria, usuarios e investigadores, es vital para el funcionamiento de los C.A.T., ya que los análisis no se circunscriben a una observación pasiva de los acontecimientos, si no que existe una actuación proactiva en la que se investigan las posibles vulnerabilidades que puede presentar un sistema así como la elaboración de un plan de sondeos a distintas organizaciones para conocer el estado actual de la seguridad informática y la repercusión que ha tenido un incidente concreto.

196

## CENTROS DE ALERTA TECNOLÓGICA EN ESPAÑA

Básicamente, en España existe un C.A.T. que unifica los esfuerzos de varias organizaciones y que fue inaugurado en Julio de 2001 llamado Centro de Alerta Antivirus ([www.alerta-antivirus.es](http://www.alerta-antivirus.es)), gestionado por la institución RED.ES, adscrita al Ministerio de Ciencia y Tecnología.

Este Centro cuenta con la colaboración del Ministerio de Administraciones Públicas y el Ministerio del Interior, con el Cuerpo Nacional de Policía y la Guardia Civil, la comunidad Universitaria e investigadora a través de REDIRIS, las empresas fabricantes de Antivirus y de seguridad informática, la Asociación Española de Empresas de Tecnologías de la Información (Sedisi) y las principales asociaciones de usuarios de Internet y la Asociación de Internautas.

Esta sinergia de esfuerzos se manifiesta en la publicación de un boletín diario en la página web del CAT donde se informa los principales peligros, noticias y soluciones a los problemas de seguridad de la Red. También los medios de comunicación televisivos colaboran con sus respectivas secciones en Teletexto.

También se ofrece información estadística en tiempo real sobre la propagación de los virus.

Además del factor preventivo, se ofrece una sección donde poder denunciar los posibles delitos con referencias al Cuerpo Nacional de Policía y Guardia Civil.

Una de las principales fuentes de información de Alerta Antivirus la constituye la cadena de observatorios formada por universidades españolas que se han ido adhiriendo al proyecto como la reciente incorporación de la Universidad de las Palmas de Gran Canaria. Actualmente esta cadena la forman 32 universidades de todo el territorio Nacional.

### **SISTEMA DE PREVENCIÓN DE DELITOS TECNOLÓGICOS EN LA POLICIA ESPAÑOLA. ALERTA 24 HORAS.**

La Dirección General de la Policía, a través de la Comisaría General de Policía Judicial, ha puesto en funcionamiento un servicio de atención de urgencia ante alarmas tecnológicas que pudieran producirse (delitos informáticos o en los sistemas de información) a fin de facilitar un punto de contacto policial que permita una reacción rápida y eficaz en la investigación y en la prevención de consecuencias (aproximación al ciudadano).

En el tiempo que lleva funcionando este servicio, se han recibido multitud de consultas en relación a delitos tecnológicos, siendo en su mayoría comunicaciones sobre sitios donde se ofrece pornografía infantil o se cometen fraudes.

Dicho servicio, se fija en el CENCI (Centro Nacional de Comunicaciones Internacionales).

Servicio de alerta tecnológica (24 horas 365 días): 91 582 29 00

Además, se establecen los canales de comunicación con la Brigada de Investigación Tecnológica.

SERVICIO	CORREO ELECTRONICO	TELÉFONOS	FAX
<b>Delitos cibernéticos</b>	delitos.tecnologicos@policia.es	91-582.27.51	91-582.27.56
<b>Pornografía infantil</b>	denuncias.pornografia.infantil@policia.es	91-582.27.53 91-582.27.54	91-582.27.56
<b>Fraudes a las Telecomunicaciones</b>	dco@dgp.mir.es	91-582.23.07	91-582.27.56
<b>Seguridad Lógica, intrusiones</b>	seguridad.logica@policia.es	91-582.27.52	91-582.27.56



## LA COLABORACIÓN INTERNACIONAL

A principios de este año, la Comisión Europea presentó una propuesta de reglamento para reforzar la seguridad informática en la Unión Europea con la creación de la Unidad de Seguridad de Redes y de la Información a nivel Europeo.

Básicamente se trata de unificar los distintos Centros de Alerta Tecnológica de los países miembros con el fin de impulsar las iniciativas de cooperación entre los distintos agentes del campo de la seguridad informática para fomentar una red más segura, sobre todo en el ámbito empresarial y conseguir un despegue definitivo del comercio electrónico.

A nivel policial, existen diversos organismos de cooperación entre los distintos países:

INTERPOL. Con la creación de las Working Party on IT Crimes en las distintas regiones del mundo, que en Europa va por la reunión número 39, se establecen unos grupos de trabajo interdisciplinarios para fomentar el intercambio de conocimientos en la lucha contra el cibercrimen. El mayor logro de esta iniciativa es la elaboración de un extenso manual en CDROM que en breve estará disponible en formato HTML en la página web de INTERPOL. Este manual está continuamente revisado y alerta sobre los posibles peligros de la Red y cómo combatirlos.

198

Europol. En esta institución, se partió de la lucha contra la pornografía infantil en Internet y se ha ido ampliando con la creación de un Grupo de Expertos en Cibercrimen a otro tipo de delitos. Europol ha elaborado un documento sobre las nuevas amenazas en los delitos tecnológicos que está siendo revisado en este momento en el seno de los países miembros.

G8. En 1997 crea el subgrupo "High Tech Crime" con un plan de acción que obliga a los miembros a establecer un punto de contacto "24/7" para la formación del personal investigador, revisión del sistema legal e intercambio de información entre países.

Otras iniciativas. A nivel particular, y con el apoyo de las anteriores, han aparecido grupos de colaboración internacional a nivel policial para el intercambio de información técnica entre investigadores. Ejemplos de ellos están los grupos:

ULLE: foro de discusión en delitos de pornografía infantil

Hannover Group:VPN destinada a la lucha contra la delincuencia tecnológica. Los países miembros de esta red y Europol han creado una infraestructura de ordenadores donde se ofrecen todo tipo de servicios, desde intercambio de mensajes hasta una base de datos de manuales o una red de ordenadores que trabajan en conjunto para romper contraseñas.



## CENTROS DE ALERTA EN ESPAÑA

### **Centro de Alertas del MAP**

<http://www.map.es/csi/pg7060.htm>

### **Servicio de seguridad IRIS-CERT**

<http://www.rediris.es/cert>

Para detección de problemas de seguridad en centros de Red-IRIS y actuación coordinada para resolverlos

### **Universidad Politécnica de Cataluña**

<http://escert.upc.es>

EsCERT-UPC, asesora en cuestiones de seguridad informática. Cuenta con mirrors cada dos días a los principales CERT y una amplia gama de artículos, documentos y enlaces

## CENTROS DE ALERTA FUERA DE ESPAÑA

### **CERT americano**

<http://www.cert.org>

(Computer Emergency Response Team): Organismo creado en 1998 por el gobierno norteamericano con el fin de servir de punto de coordinación entre fabricantes y usuarios, para obtener soluciones en temas de seguridad en Internet (en inglés).

199

### **CERT europeo**

<http://www.eurocert.net>

European Security Incident Information Service (en inglés).

### **AusCERT**

<http://www.auscert.org.au>

Australian Computer Emergency Response Team (en inglés).

### **DFN-CERT**

<http://www.cert.dfn.de>

Computer Emergency Response Team for the German Research Network DFN and its services (en alemán e inglés).

### **FIRST**

<http://www.first.org>

Forum of Incident Response and Security Teams(en inglés).

### **CSRC**

<http://csrc.nist.gov>

Computer Security Resource Center. Información mantenida por NIST (en inglés).

**CIAC**

<http://www.ciac.org>

Computer Incident Advisor Capability (Departamento de Energía de EEUU) con información sobre varios temas de seguridad: virus, falsos virus, programas antivirus, etc. (en inglés).

**CSIRT**

<http://www.csirt.co.uk>

Computer Security Incident Response Team (en inglés).

**FedCIRC**

<http://www.fedcirc.gov>

Federal Computer Incident Response Capability (en inglés).

# PROTECCIÓN DE LA TECNOLOGÍA

**Javier Pericacho Sastre**  
**Inspector Jefe del Cuerpo Nacional**  
**de Policía**

## INTRODUCCIÓN

Vamos a tratar la realidad y el problema de la protección de la tecnología si bien bajo la óptica de la Comisaría General de Información -CGI-, es decir especialmente referida a tecnologías sensibles y en el marco de la defensa de los intereses económicos y de seguridad nacionales.

201

Para ir situándonos en el entorno de esta realidad actual que, aunque el ciudadano medio y el empresariado en general desconoce casi totalmente y lo ve como algo de cine o novelesco, existe toda una gama de vocablos que a menudo se refieren al tema objeto del presente trabajo y nos da una idea de la enjundia del tema en cuestión.

Nos referimos a términos como opacidad, apantallamiento, camuflaje, solapamiento, sutileza, subrepticia, sustracción, amenaza, coacción, chantaje...etc.

Bien, si hablamos de protección de la tecnología lo primero y obligado será conocer y saber qué entendemos por tecnología.

## TECNOLOGÍA

Desde que surge la idea en el empresario de producir algo hasta que aparece el artículo u objeto, al final de la cadena de producción, existe todo un proceso industrial que abarca diversas etapas como desarrollo, producción, utilización, etc. y conlleva además la conjunción de diversos aspectos



y actividades como: idea, diseño, planos, ingeniería, equipos, instalaciones, personas...etc.

Pues bien, solo a una parte de ese proceso industrial es a lo que se denomina tecnología y no es más que: "la información específica requerida para el desarrollo, producción y/o utilización de un producto". Es decir la información de cómo desarrollar, cómo producir y cómo utilizar el producto en cuestión.

### Importancia de la Tecnología

El mayor activo de una empresa es su información tecnológica, su tecnología propia y específica. Si la pierde o le es sustraída esa empresa está abocada al fracaso y posiblemente a su fin.

En este contexto, algún analista ha publicado que la pérdida de propiedad intelectual, información tecnológica y de otros aspectos intangibles le cuesta cada año a las compañías por lo menos un 6% de sus ingresos totales anuales.

Si convenimos que la tecnología es un activo empresarial vital, hemos de añadir que, precisamente por esa razón, es apetecida por empresas de la competencia, por personas "encomendadas, dispuestas y especialmente entrenadas" para la adquisición y sustracción de tecnología, por oscuras organizaciones e incluso por determinados países, con una u otra razón más o menos confesable.

El enemigo al que se enfrenta la tecnología es el espionaje industrial. Así que, para mejor combatirlo, hay que conocerlo previamente.

## ESPIONAJE INDUSTRIAL

Conviene significar que, en el panorama del espionaje mundial y desde la década de los 90, los objetivos políticos y militares han dejado de ser prioritarios, han sido desplazados a un segundo lugar. Tras el reciclaje pertinente en cuanto a estrategias y objetivos, ahora interesan más los secretos industriales.

Ciertamente en la actualidad, el espionaje industrial tiene más fuerza y pujanza que el espionaje político y el militar.

Por poner un ejemplo, hoy no interesa tanto conocer el número de aviones de guerra que pueda tener un determinado país cuanto la forma y modo de fabricarlo, es decir su tecnología. De hecho, se observa palpablemente que, hoy día, muchos países y empresas intentan adquirir tecnologías antes que sistemas acabados.

## ¿Qué ha propiciado el espionaje industrial?

En la sociedad industrial actual, la mera fórmula de un nuevo producto no conlleva el éxito, como ocurría en la sociedad industrial anterior, sino también la venta, la distribución, la marca, la campaña publicitaria, el listado de clientes, etc. Todo ello ha traído consigo la variedad de factores que inciden en el éxito de un producto y por consiguiente la multiplicidad de objetivos a investigar, atacar o espiar. En definitiva, la propia evolución industrial y tecnológica ha propiciado el espionaje industrial.

Así pues, al nuevo espionaje le interesa conocer los secretos industriales, la capacidad científica y tecnológica de otros países o empresas competidoras; le interesa conocer la razón de una determinada eficacia en la producción, le interesa conocer estrategias comerciales, listas de clientes preferentes, fórmulas de financiación, campañas publicitarias, etc.

Podemos afirmar que, en el tercer milenio, las actividades de espionaje industrial se han convertido:

- en algo relativamente cotidiano en el mundo de las empresas
- en un objetivo prioritario para distintas agencias o gabinetes de inteligencia.

203

## Objetivo

El objetivo principal del espionaje industrial es ahorrarse el coste de la investigación y de los ensayos que conllevan los nuevos productos y tecnologías. En definitiva, conseguir información que dé como resultado una ventaja económica, industrial, comercial, tecnológica o financiera.

Como ya hemos dicho, el espía industrial no sólo persigue fórmulas de productos sino también diseños, procesos de fabricación, resultados de ensayos, acuerdos financieros, formas de financiación, listas de clientes, proveedores, proyectos, nombres de ejecutivos y técnicos, etc.

## Característica

Una de las características más importante y específica del espionaje industrial es que, a diferencia del robo o el hurto, la sustracción de tecnología pasa, con frecuencia, desapercibida durante un largo tiempo. Un documento puede fotografiarse sin dejar rastro y pasar tiempo hasta darse cuenta la empresa que ha sido víctima de esa sustracción de información.

Contrariamente a los terroristas, que a menudo buscan publicidad y reivindican sin tardanza la responsabilidad de sus actos terroristas, el espía industrial se emplea a fondo en su anonimato y en camuflar o solapar sus actividades.

Esta gran diferencia nos lleva a algunas conclusiones:

- Los espías industriales son mucho más difíciles de detectar y detener.
- El público, en general, no lee nada de ellos en la prensa diaria.
- El descubrimiento de las actividades del espía industrial se realiza con cierta posteridad e incluso pasan años sin ser apercibidas.

## CAUCES Y HERRAMIENTAS

### Faceta humana

La mayor parte de las veces, el espionaje industrial se realiza aprovechando una o varias deficiencias o fallos humanos: la traición, la indiscreción o la negligencia.

La Traición entendida como la acción de entregar al adversario la información tecnológica de la empresa.

Puede estar motivada por el afán de lucro, motivos personales y bajo coacción

204

Es necesario prestar atención a las personas consideradas “vulnerables”, es decir aquel empleado o directivo con acceso a información sensible que pueda ser objeto de chantaje por cualquier circunstancia personal, familiar, política o social. Por esta razón, las personas consideradas vulnerables no han de tener acceso a información sensible.

La Negligencia. Se trata de la participación inconsciente del sujeto en la entrega de la información. Es la antesala del espionaje. Va unida habitualmente a la incredulidad respecto a la necesidad de proteger la tecnología y a una peligrosa inconsciencia profesional. Un ejemplo es dejar abiertos los archivos, olvidar o perder documentos, admitir visitas en zonas restringidas...

La Indiscreción se diferencia de la negligencia en que supone un mínimo de participación activa por parte de su autor. Es consecuencia de la falta de conciencia y mentalización respecto a la importancia de salvaguardar la tecnología de la propia empresa. Otro ejemplo con indiscreciones en charlas amistosas, en locales de ocio, con un amigo de “confianza”, etc.



## FACETA TÉCNICA

El espía industrial puede utilizar múltiples y variados recursos técnicos de teleinformática, telecomunicación y teleinformación. Se dice que muchos de estos recursos o ayudas técnicas no son mas que una prolongación de uno o varios de los sentidos corporales. Y así, las cámaras de fotografiado y sistemas de filmación serían la prolongación de la vista, los micrófonos y sistemas de captación del sonido lo serían del oído, etc.

A lo anterior hay que añadir que el espía industrial puede utilizar, para lograr sus objetivos, distintos:

### **Procedimientos**

Soborno  
Chantaje  
Intercepción de sonido telefónico o ambiental  
Filmaciones  
Sexo, vanidad  
Etc.

### **Formas**

Desde dentro de la empresa  
Desde fuera (intrusión)  
Etc.

### **Coartadas**

Publicitario  
Reportero  
Inspector de calidad o medidas de prevención  
Aparente visita comercial  
Aparente entrevista de trabajo o caza-talentos  
Etc.

## PROTECCIÓN DE LA TECNOLOGÍA

Si hemos asumido la importancia que tiene la tecnología, hemos observado que es “especialmente apetecida y objeto de deseo en cualquier forma y modo” y conocemos ya quien y cómo es su verdadero “enemigo” -el espionaje industrial-, hay que convenir la necesidad imperiosa de proceder a su protección.

### **Finalidad de la protección**

Consiste en impedir fugas de información tecnológica a empresas o países directamente competidores y más aún, desde la óptica de la Dirección General de la Policía - Comisaría General de Información, especialmente que esas fugas puedan ir a países considerados sensibles en el ámbito de la proliferación armamentística.

También en lograr la seguridad industrial integral, mediante la conjunción de:

- Seguridad de las Instalaciones
- Seguridad de las Personas
- Seguridad de la Tecnología

## HERRAMIENTAS DE PROTECCIÓN

### Por parte de le empresa

La implantación de un verdadero Plan de Seguridad Industrial (PSI) en el marco de la seguridad industrial.

La disposición de un gabinete de inteligencia empresarial, encargado de evaluar y detectar las fallas, carencias y vulnerabilidades de seguridad tecnológica en la propia empresa así como las de la competencia.

206 Este Gabinete captará y reunirá información al mismo tiempo sobre el “saber hacer” (know how) o conocimiento ajeno, para aplicarlo en provecho de la propia empresa. Por todo ello habrá de contar con los conocimientos adecuados de espionaje, contraespionaje y seguridad Industrial.

Conviene aclarar que la inteligencia empresarial, totalmente lícita, sólo se diferencia del espionaje industrial en los métodos empleados.

No obstante, muy pocas empresas españolas han aprendido a usar esta poderosa arma.

### Por parte de la Dirección General de la Policía - Comisaría General de Información

Plan de Alerta y Concienciación a las empresas, sobre la materia objeto del presente trabajo, con una labor de apoyo y asesoramiento en la implantación de sus Planes de Seguridad.

Control de la transferencia de tecnología especialmente referido a tecnologías sensibles, tanto en su forma tangible como intangible.

Hay que señalar que estas herramientas o instrumentos de protección engloban y complementan toda una serie de principios básicos y técnicas de contraespionaje que ayudan a prevenir las fugas de la información tecnológica y, en definitiva, a salvaguardar la información sensible de la empresa.

## **Relevancia de la protección tecnológica**

Para la Comisaría General de Información, en el marco en que nos movemos de defensa de los intereses económicos y de seguridad nacionales, la protección de la tecnología es un objetivo estratégico de prioridad.

Hay que significar que, muy a menudo y muy actualmente, la transferencia o exportación indebida de tecnología es el factor más importante para el desarrollo de armas de destrucción masiva -ADM- o NBQ.

Por tanto, si protegemos la tecnología evitando fugas de información tecnológica, sobre todo cuando hablamos de tecnologías sensibles y precisamente que vayan a parar a países considerados proliferantes o de preocupación, evitamos de alguna forma la proliferación de armas de destrucción masiva. Y si evitamos la Proliferación de ADM evitamos al mismo tiempo que el terrorismo NBQ pueda tener acceso a esas armas de destrucción masiva.



## ANEXO

### PRINCIPIOS BÁSICOS Y TÉCNICAS DE CONTRAESPIONAJE INDUSTRIAL

Creación de un Departamento de Seguridad Industrial e Inteligencia Empresarial.

Elaboración de un Plan de Seguridad Industrial –PSI–.

Asignación de un presupuesto real a la seguridad e inteligencia empresarial.

Concienciación del personal (directivos y subalternos) de la necesidad de proteger la tecnología.

Localización y ubicación de la “información sensible”. Para mejor proteger la tecnología, previamente hay que determinar dónde se encuentra.

208 Utilización de técnicas de selección del personal que vaya a tener acceso a información sensible.

Prestar especial atención, por el Departamento de Seguridad Industrial e Inteligencia Empresarial, al personal vulnerable.

Discreción extrema en función de determinados lugares, temas de conversación y documentos que se porten.

Exigencia de contratos de confidencialidad al personal que conozca o vaya a manejar información sensible de la empresa.

Clasificación y protección de la información sensible. Niveles de acceso, custodia, traslado, remisión, entrega, utilización, copiado, fotocopiado o destrucción.

Atención a las empresas de mantenimiento y de subcontratación, vía utilizada a menudo por el espionaje industrial.

Realización de “Barridos electrónicos” periódicos, especialmente en las salas de reunión de los directivos y ejecutivos.

Protección de las comunicaciones telefónicas: secrafonías, etc.

Protección del correo electrónico.

Codificación de vídeo, tanto las señales de audio como las de imagen, especialmente de las teleconferencias inter-directivos.

Codificación informática.

Atención a simposios, exposiciones y presentaciones comerciales. Evitar situaciones comprometidas que puedan convertirnos en “personal vulnerable”.

Oficinas ejecutivas y de ingeniería cerradas cuando no se utilicen, o en ausencia del operario.

Evitar la desafección, caldo de cultivo para el espionaje industrial.



## COLOFÓN



## COLOFÓN

**Isaac Martín Barbero**  
**Director del Seminario**

A lo largo de las últimas décadas, las sociedades avanzadas han pasado a asentarse sobre el conocimiento y la información. En nuestro tiempo, el desarrollo social y personal depende, sobre todo, de la capacidad de procesar y transportar información con rapidez y precisión. La información constituye el nexo fundamental de los miembros de la sociedad global y el elemento que ha hecho compatible la diversidad de entornos físicos con la existencia de una única megalópolis virtual.

213

Las aportaciones que se recogen en este libro ponen de manifiesto que tal y como señalan Davenport y Prusak(1), información es la suma de datos y significado y que estamos aun en una etapa del desarrollo de la Sociedad de la Información, que cabe caracterizar como la era de la tecnología de la información.

Conviene que no perdamos de vista que lo que llamamos "Sociedad de la Información" es ante todo "Sociedad" y como tal, está constituida por personas para quienes cultura y contexto siguen siendo esenciales. En concreto, la "cultura" resulta fundamental para garantizar que la Sociedad de la Información sea también una Sociedad de Conocimiento, donde la información sea un instrumento básico de capacitación de la humanidad. Entonces, la persona amparada en sus valores y creencias protagonizará este tránsito desde la información hasta el conocimiento cuando se aplique a organizar, elegir, aprender o juzgar. Sin embargo, el elemento humano, piedra angular de las magníficas potencialidades que nos ofrecen las nuevas tecnologías, también constituye su mayor amenaza cuando se apliquen éstas a la desestabilización y al crimen.

---

1.- Davenport, T. & Prusak, L. (1998). "Working knowledge". Cambridge MA: Harvard University Press.

Frente a esta realidad, los gestores de la seguridad han de mantenerse en vanguardia de la gestión del conocimiento con la ventaja de partida que les otorga su condición de expertos en las relaciones humanas. Los nuevos profesionales de la seguridad han de ser capaces de participar e influir sobre los cambios que se producirán en las organizaciones y la sociedad. Como profesionales del conocimiento, que siempre fueron, han de saber servirse de las contribuciones que la tecnología de la información puede aportar a la mejor gestión social y policial y deberán responder a la creciente necesidad de compartir conocimiento con agentes de otros ámbitos geográficos y campos profesionales en la dimensión real y virtual. La Policía habrá de perseverar en su convicción de que la gestión del conocimiento no es algo que verse sobre tecnología sino que trata de personas, de prácticas de gestión y de cultura de trabajo.

El trabajo acumulado en estas aportaciones nos permite felicitarnos, estimula el esfuerzo frente a los desafíos expuestos y nos conmina a hacer frente a éstos y a los que surgirán en el futuro desde la experiencia acumulada, con la colaboración y los mejores esfuerzos de todos.