R. 30189 N. 34384

XII CONGRESO ESPAÑOL DE GERENCIA DE RIESGOS Y SEGUROS

AGERS 2000

LA AGRAVACIÓN DE LOS RIESGOS EN EL 3er MILENIO. RESPUESTAS PARA SU GESTIÓN Y FINANCIACIÓN.

29 Y 30 DE NOVIEMBRE DE 2000

ORGANIZADO POR:

AGERS

ASOCIACIÓN ESPAÑOLA DE GERENCIA DE RIESGOS Y SEGUROS

PATROCINADO POR:

AIG EUROPE

Allianz

AON *Aon Gil y Carvajal*

ASEPEYO

ESTRELLA SEGUROS

GERLING

Heath Lambert Group

MARSH An MMC Company

GENERALI GLOBAL

S&C WILLIS CORROON CORREDURIA DE SEGUROS Y REASEGUROS, S.A.

REVISS SERVICIOS INTEGRALES PARA SEGUROS

SISTEMA MAPFRE

VITALICIO SEGUROS

ZURICH

PROGRAMA

DIA 29

9:00 ACREDITACIÓN

9:30 INAUGURACIÓN

- **ILMA. SRA. DÑA. PILAR GONZÁLEZ DE FRUTOS**
  Directora General de Seguros
- **D. EDUARDO ROMERO** – Presidente de AGERS

10:00 RIESGOS DEL COMERCIO ELECTRONICO. RESPUESTA DE LA GERENCIA DE RIESGOS.

- **D. FRANÇOIS SETTEMBRINO** – Ex-presidente de FERMA , Director de Educación de FERMA.
- **D. MANUEL CARPIO** – Gerente de Seguridad Lógica de TELEFÓNICA DE ESPAÑA.
- **D. GONZALO ITURMENDI** - Abogado, Secretario General de AGERS

COLOQUIO

11:15 Café

11:45 EL CAMBIO CLIMATICO Y LA AGRAVACIÓN DE LOS RIESGOS CATASTRÓFICOS.

- **D. LUIS BALAIRÓN** – Jefe del Servicio de Variabilidad y Predición del Clima del INSTITUTO NACIONAL DE METEOROLOGÍA.
- **D. CARLOS DUEÑAS** – Vocal Asesor de la DIRECCIÓN GENERAL DE PROTECCIÓN CIVIL
- **D. JOHN FORDER** – Managing Director (Project Risks Group) HEATH LAMBERT GROUP.
- **DÑA. MAYTE PISERRA DE CASTRO** – Subdirectora del Departamento de Riesgos de la Naturaleza de MAPFRE RE.
- **DÑA. ANA GARCÍA-BARONA** - Directora Técnica y de Reaseguro del CONSORCIO DE COMPENSACIÓN DE SEGUROS

COLOQUIO

MODERADOR: **D. Ignacio Martínez de Baroja** – Consultor de Riesgos.

14:00 Almuerzo

11: 00 PANEL: VISIÓN GENERAL.
LA DISGREGACIÓN DE LOS ACTUALES PROGRAMAS DE SEGUROS.
¿Una consecuencia solapada del endurecimiento del mercado?

- **D. EDUARDO ROMERO** – Gerente de Riesgos del GRUPO DRAGADOS
- **D. ENRIQUE ZÁRRAGA** – Director General Adjunto de S&C WILLIS CORROON
- **D. ANTONIO GONZÁLEZ** - Director Unidad de Energía de AON GIL & CARVAJAL
- **DON JOSÉ ANTONIO GARCÍA** – Director División Negocio Internacional GENERALI GLOBAL
- **DON EDUARDO LLINÁS** – Director División VITALICIO SEGUROS

12:40 MESA REDONDA

MODERADOR: Don Gonzalo Fernández Isla – Gerente Desarrollo Internacional de TEFÓNICA, S.A. Vicepresidente II de AGERS.

13:15 PRESENTACIÓN GRUPO DE TRABAJO DE "RESPONSABILIDAD PATRIMONIAL DE LAS ADMINISTRACIONES PUBLICAS".

14:15 CLAUSURA

LISTA DE PARTICIPANTES

Nº	NOMBRE	EMPRESA
	AGUILAR, GONZALO	Miembro Individual de AGERS
	ALARCÓN, JOAQUÍN Director	MÜNCHENER
	ALEJANO, LUIS Jefe de Ingeniería de Riesgos	TELEFONICA, S.A.
	ANDRÉS, JUAN JAVIER Periodista	LA GACETA
	ARCELUS, CARMELO Vice-Consejero Admon. Y Servicios	CONSEJERIA DE HAC. Y ADMON. PÚBLICA GOBIERNO VASCO
	ARRIOLS, ENRIQUE Director	MARSH, S.A.
	BALAIRÓN, LUIS Ponente	INST. NAL. DE METEOROLOGÍA
	BALLESTER, VICENTE Gerente Seguros, Beneficios Sociales y Pensiones	FORD ESPAÑA, S.A.
	BASABE, LUIS Director	MARSH, S.A.
	BASALDUA, FERNANDO Gerente de Riesgos	IBERDROLA, S.A.
	BEER, ADRIÁN, Gerente	GRUPO BEER
	BELENGUER, Mª ANGELES Coordinador Area Seguridad	MERCADONA, S.A.
	BENITO, GREGORIO Ponente	CC.OO
	BEODDEUS, SANDRA Ejecutivo de Cuentas	AON GIL & CARVAJAL
	BINDELLE, FLORENCE Gerente	FERMA
	BLANCO, FERNANDO Ponente	TABACALERA ESPAÑOLA, S.A.
	BODEGAS, ROBERTO Director Comercial	MARSH, S.A.
	BYME, JOHN Director Líneas Financieras	AIG EUROPE

DOMÍNGUEZ-MACAYA, JAIME Dctor. Gral. De Patrimonio y Contratación	CONSEJ. HACIENDA Y ADMON. PÚBLICA GOBIERNO VASCO
DUEÑAS, CARLOS Vocal Asesor	DIREC. GRAL PROTECCIÓN CIVIL
ESTEBÁN DE LA ORDEN, RICARDO Gerente de Riesgos	FERROVIAL AGROMAN, S.A.
ESTIRADO, SARA Asesor Técnico de Riesgos	INDEPENDENT INSURANCE
FAJARDO, PAULINO, Ponente	DAVIS ARNOLD COOPER
FERNÁNDEZ, AGUSTÍN Grupo I, N1, Apoderado	WINTERTHUR IBERICA, AELE
FERNÁNDEZ, GONZALO Moderador	TELEFONICA, S.A.
FERNÁNDEZ, JOSE RAMÓN Administración de Seguros	HIDROELECTRICA DEL CANTABRICO
FONTANILLA, OLIVIA Periodista	LA GACETA
FORDER, JOHN Ponente	HEATH LAMBERT GROUP
GALLEGO, ALBERTO Director General	S& C
GARCÍA-OREA, ALVARO Ponente	FCC
GARCIA, ANA Ponente	CONSORCIO COMPENSACIÓN DE SEGUROS
GARCIA, FERNANDO Resp. Decenal – R. Técnicos	GE FRANKONA RE
GARCÍA, JOSÉ A. Ponente	GENERALI GLOBAL
GARCÍA, JUAN ALBERTO Ejecutivo de Cuentas Internacionales	MAPFRE CONSULTORES
GARCÍA, JULIÁN Ejecutivo de Cuentas División Gerencia de Riesgos	CENTRO DE SEGUROS EL CORTE INGLÉS
GARCÍA, JULIO Ejecutivo de Cuentas	S&C
GARCÍA, MAITE	AGERS
GARCIA DE ANDOAIN, CARLOS Director U.E.	PLUS ULTRA

GARRIDO, RICARDO Abogado	DAVIES ARNOLD COOPER
GARROTE, MANUEL Jefe de Servicios de Seguros	OHL
GIRALDA, VICTORIANO Resp. Zona Noreste y Negocio Insular	ENDESA
GOLDING, MICHAEL Director General	MARSH, S.A.
GONZÁLEZ, ALBERTO Presidente	IBERSEGUROS
GONZÁLEZ, ANTONIO Ponente	AON GIL & CARVAJAL
GONZÁLEZ, LUIS Ponente	ASEPEYO
GONZÁLEZ DE FRUTOS, PILAR Directora General de Seguros	DIRECCIÓN GENERAL DE SEGUROS
GRANDAL, LUIS Periodista	
IBAÑEZ, JOSÉ LUIS Adjunto a la Dirección Comercial	MAPFRE INDUSTRIAL
ITURMENDI, GONZALO Abogado, Secretario General de AGERS	BUFETE ITURMENDI
JIMENEZ-TAZA, PEDRO Corredor de Seguros	
LAMET, MIGUEL ANGEL Presidente	COMISMAR
LARRAT, CARLOS Responsable sector Seguros	ITSEMAP
LÓPEZ, ALVARO Master Gerencia de Riesgos	FUNDACIÓN MAPFRE ESTUDIOS
LOSADA, JAVIER Gerencia de Riesgos	INDITEX, S.A.
LLINÁS, EDUARDO Ponente	VITALICIO SEGUROS
MACIAS, MIGUEL ANGEL Director Dpto. Seguros	FCC, S.A.
MARICQ, IVAN Consultor	GLOBAL INSURANCE SERVICES, S.L.
MARIN, ANTONIO MANUEL Corredor de Seguros	

MARTÍN, VICENTE Gestor Adjunto Riesgos de Patrimonio	ENDESA
MARTÍNEZ, FRANCISCO Director ISI	FUNDACIÓN MAPFRE ESTUDIOS
MARTÍNEZ, IGNACIO Director de Grandes Cuentas	ALLIANZ
MARTÍNEZ DE BAROJA, IGNACIO Moderador	CONSULTOR DE RIESGOS
MARHUENDA, MERCEDES Coordinadora de Zona	REVSIS
MATA Y GALÁN, SEBASTIÁN Gerente	IBERSEGUROS
MARTÍNEZ, VISITACIÓN Directora General de Patrimonio	CONSEJERÍA DE ECONOMÍA Y HACIENDA REGIÓN DE MURCIA
MATAMOROS, BERNARDO Suscriptor de Reaseguros	GERLING GLOBAL REASEGUROS, S.A.
MENDEZ, JOSÉ ANTONIO Dctor. Serv. Direcc. C. Financ. de Seguros	CIMPOR
MENDIALDUA, IGNACIO Subdirector General	EUROBROK, S.A.
MENENDEZ, JOSÉ RAMÓN Director de IB	AON GIL& CARVAJAL
MOLINERO, LUIS	DIRECCIÓN GENERAL DE PATRIMONIO COMUNIDAD AUTÓNOMA DE MADRID
MONEDERO, JUAN CARLOS Subdirector	AXA SEGUROS
MONTESINOS, ANGEL Director	TOPLIS AND HARDING ESPAÑA
MORALES, CESAR Master Gerencia de Riesgos	FUNDACIÓN MAPFRE ESTUDIOS
MOTAS, PEDRO Jefe de Sección Gestión de Riesgos	CONSEJERIA DE ECONOMÍA Y HACIENDA REGIÓN DE MURCIA.
MUCCI, MARCO Director Comercial	AIG EUROPE
MUÑOZ, PAUL Master Gerencia de Riesgos	FUNDACIÓN MAPFRE ESTUDIOS
ORTÍZ, LUIS Ponente	ZURICH
PALACIOS, CARMEN Directora General	BARCLAYS CORREDURIA

PAREJA, RODRIGO Periodista	FORMACIÓN DE SEGURIDAD LABORAL
PÉREZ, FERNANDO Gerencia de Riesgos	INDITEX, S.A.
PEREZ, SUSANA Directora de Formación	INESE
PISERRA DE CASTRO, MAYTE Ponente	MAPFRE RE
POMATTA, ROBERTO L. Director Técnico	ASIRIS, S.A. CORREDURIA DE SEGUROS
PRIETO, MERCEDES Gerente	AGERS
PRIETO, MIGUEL	ADECOSE
QUIROS, ENRIQUE Director	HEATH LAMBERT Y ASOCIADOS, S.A.
REED, MICHAEL Ponente	MARSH, S.A.
REVSIS	
RIOS, CARLOS Director Riesgos y Seguros	ENDESA
RODRÍGUEZ, ALFREDO Responsable Salvación y Recuperación	GRUPO BEER
RODRÍGUEZ, CESAR Director de Riesgos y Seguros	VALENCIANA DE CEMENTOS
RODRÍGUEZ, ELIAS Director General	CRAWFORD & COMPANY
RODRÍGUEZ, JOSE CARLOS Director General	MARSH, S.A.
RODRÍGUEZ, LUIS Master Gerencia de Riesgos	FUNDACIÓN MAPFRE ESTUDIOS
RODRÍGUEZ, MIGUEL Director	GERLING-KONCERN
ROMANILLOS, TOMÁS	Miembro Honorario de AGERS
ROMERO, EDUARDO Presidente de AGERS	GRUPO DRAGADOS
RUIZ DE LA SERNA, Abogado	BUFETE ITURMENDI
SÁEZ, JULIO Moderador	C.S. EL CORTE INGLES

SAÉZ, ANTONIO Dctor. Ctas. Des. Negocio Area Centro-Sur	AON GIL & CARVAJAL
SANCHEZ, JOSÉ LUIS Consejero Delegado	ASEVASA
SANZ, JOSE MANUEL Director Técnico	CORREDURIA SEGUROS G. BAYLIN
SANZ, RICARDO Director	AON & GIL & CARVAJAL
SCHOCH, ENRIQUE Dctor. Desarrollo División Broker	ROYAL SUN ALLIANZA
SETTEMBRINO, FRANÇOIS Director de Educación	FERMA
SILVA, FERNANDO Jefe Dpto. Seguros	FCC, S.A.
SOLER, JULIA Jefe del Serv. de Gestión y Prevención De Riesgos, Dpto. Economía y Finanzas	GENERALITAT DE CATALUNYA
TOMEY, PEDRO Director Comercial	AON GIL& CARVAJAL
TORRE, TOMÁS Gerente	ASEVASA
TORRES, JUAN ADOLFO Ingeniero Consultor	VALUATION CONSULTING GROUP, S.A.
VALENTÍN, CANDIDO Director Financiero	OHL
VARELA, FERNANDO MANUEL Master Gerencia de Riesgos	FUNDACIÓN MAPFRE ESTUDIOS
VASQUEZ, CARLOS Consejero Delegado	HEATH LAMBERT Y ASOCIADOS, S.A.
VIVAS, MANUEL Director	ALEXANDER FORBES
WESOLOWSKI, PABLO Socio-Director	DAVIES ARNOLD COOPER
ZAMORA, ROMULO Director Ocio y Turismo	AON GIL & CARVAJAL
ZÁRRAGA, ENRIQUE Ponente	S&C WILLIS CORROON

AGERS CONFERENCE

MADRID, 29/30 November, 2000

CYBER-RISKS

Introduction by F. Settembrino

The following ideas are expressed from a Risk Management point of view:

a) Risk Management, the systemic approach; (not the holistic one)

Every company or organisation is a "system" this means that all components are to be taken into consideration, with their interrelations.

A system is never insulated from the external world. It constitutes an "ensemble or coherent set", which can be considered as a "sub-set" linked with many others.

The main problem comes from the fact that two aspects of the Risk may cause problem. On one side all the risks being not-identified or not-identifiable and on the other side, not all the risks are quantifiable, (e.g. image, reputation).

One should not forget that the terminology is not yet universal. The word Risk can cover damages, a dimension of damages, or the variance of probabilities, including profitable issues.

b) Applied to cyber-risks, what are the major components of Risk;

Instead of reproducing an extensive dictionary, we can limit our set of risky components to three main categories;

- First, the physical aspects. The machines and machinery, the interconnection facilities, including all electronic devices and networking.
- Secondly, all the legal aspects, including existing rules, intellectual property safeguards, commercial and contractual agreements... and liabilities.
- Thirdly, ethics. They cover not only the aspects related to privacy protection, but include the so numerous no-discrimination laws and guidelines. decency, children's protection etc.

A few are difficult to classify, like image, reputation, brand value, and so on.

c) Are those risks manageable?

The answer is "yes and no" because we suffer a lack of past experience. Let us take the Y2K solving as a positive example:

- We learned that the dimension of the Y2K problem was enormous, and was not restricted to the machinery itself, because of the interdependence with the supply chain (goods, energy, communications...), with the warehousing and with the distribution chain. Only an extraordinary exchange of information between the factors and between the actors avoided the major consequences of the simple change of date. The exercise has shown that the magnitude of the problem was much bigger than expected. Finally, it has been overcome due to combined efforts of many.

- From the "I love you" virus recent contamination we experienced the fragility of the net. Experts never agree on the number and types of the aggression mechanisms, but generally they promise a lot of disagreeable discoveries in the coming months and years. The inventivity of the aggressors is improving at a higher speed that the protection systems we try to install. With great efforts and competency we can reach, but will never attain full protection, the aim is to attain a sufficient level, keeping in mind that the zero Risk is an utopia!.

To feed some reflection and curiosity, let me give you a few examples of a possible future evolution. It could be that instead of using telephone or similar networking, the net connections could go through the electrical cables. (That possibility exists already since years for babyphones). It is also question to make all the cable spaghetti and infrared connections between printers, scanners, cameras, projectors and any P.C. completely obsolete and to replace them by radio chips. Bluetooth is the new name, it works with a very low power, and is thus only usable in restricted areas, and today for a maximum of eight devices.

An other example of new danger can be found in the so called "web bugs": generally all organisations working or selling on the web do use common navigators, in the hands of commercial agencies. Some time ago, in one article, I focused on the "cookies" malicious aspects. Those cookies, at each visit on the site, unveil secretly address and identification of the visitor.

A web bug is slightly different, in the sense it is disseminated under the form of an invisible image of a 1/1 pixel size. That image is hidden in one or several pages. All readers of any HTML mail do identify themselves: the server repatriates than the small web bug from the computer of the reader, and so can identify and retain the transmitter`s location, with name and address. Mixing the data, with those already given by any cookie, they may build a comprehensive nominate data base. Any further connection becomes not anonymous anymore. I give you this as an example already known, but for sure, many other forms of espionage do exist, increasing vulnerabilities at any level. Even the US Pentagon is conscious of the problem.

For more information, visit the following sites:

- www.cnil.fr/traces
- www.cookiecentral.com
- www.tiac.net/users/smiths/privacy/wbfaq.htm
- www.dejanews.com

The conclusion: we need meetings like this conference to improve our knowledge and improve our Risk Management abilities. The other speakers will contribute to... We also need the expertise of our own specialised technicians and we need the collaboration of all members and employees within our companies and organisations. We may count on the assistance of our national and international clubs, together with our industrial, and professional unions, their actions are dedicated to the solution of the problem, or at least to the understanding and protecting aspects. What is more difficult, even if it is essential for an appropriate Risk Management handling, is to obtain full understanding of the magnitude of the problem from the Board and from the Top Management. However, it is part of their Corporate Governance duty.....

¿Es posible la gestión de e-Riesgos?

Resumen

Existen desde hace tiempo soluciones tecnológicas capaces de hacer viable un comercio electrónico seguro a través de una red abierta como Internet. Sin embargo las administraciones públicas y muchas empresas presentan aún inercias respectivamente en el desarrollo del marco legislativo y en la adopción de un claro compromiso inversor en seguridad. La seguridad total nunca será posible, de manera que el riesgo residual deberá ser transferido.

La seguridad en Internet... o de cómo convertir la amenaza en oportunidad

La red Internet ya se ha convertido en el sistema nervioso de laTierra, permitiendo comunicación casi instantánea entre todos sus usuarios, acceso a prácticamente todo conocimiento existente, y la implementación de aplicaciones que prometen revolucionar muchos de los quehaceres humanos, incluyendo la educación, los medios de comunicación, los servicios bancarios, la compra-venta de productos y servicios, las telecomunicaciones, la publicación de obras originales, la publicidad comercial, etc. Virtualmente en todas esas aplicaciones, la seguridad representa un parámetro central para su diseño y efectividad. Sin embargo, el crecimiento explosivo y desordenado de Internet, la oferta de múltiples soluciones y "estándares" para la seguridad, y el hecho de que la mayoría de los países avanzados en este campo prohiben la exportación de fuerte
encriptación, han generado un ambiente de confusión en el usuario final y en los gerentes que toman decisiones sobre cómo integrar Internet en su negocio u organización.

Afirmar que "Internet es una red insegura" tiene tanto sentido como decir que el idioma español es inseguro. Internet es un medio de comunicación, y como tal su grado de seguridad dependerá de la voluntad y la capacidad inversora de quien lo quiera utilizar para sus transacciones. Lo que puede ser seguro o inseguro es la manera de implementar comunicaciones en este medio. Por un lado, el aspecto global de Internet y el hecho de que los paquetes IP se transportan de una manera autónoma hace que datos enviados por Internet se pueden interceptar por personas no autorizadas. Es cierto entonces que los datos enviados por Internet no están seguros. Lo mismo, en mayor o menor grado, es cierto sobre toda comunicación a larga distancia, sea por teléfono, correo postal, telegrama o radio. Por otro lado, el hecho de que Internet es una red de ordenadores donde todos los datos se representan como datos digitales permite lograr un grado muy alto de seguridad que no es posible o muy difícil lograr con otros medios.

La evolución de las nuevas tecnologías, en especial el tremendo auge de las tecnologías Internet/Intranet, ha provocado la aparición de nuevas necesidades y la posibilidad de adquirir ventajas competitivas. Además hay que aclarar que lo que inicialmente partió como una opción de negocio se está transformando en una elección obligada si se desea mantener la posición en el mercado frente a los
competidores; así, hasta los más reacios han debido claudicar ante la evidencia aplastante.

Los beneficios atribuibles a las nuevas tecnologías son muchos, pero también los riesgos: La pérdida de imagen (a menudo más crítica que la propia perdida de datos), la perdida de información, la suplantación de usuarios, el espionaje de información sensible o incluso el cumplimiento de la normativa vigente..

A pesar de lo cambiante del entorno, los requisitos de seguridad siguen siendo los mismos: Autenticación, confidencialidad, control de acceso, integridad y no repudio; aunque los objetivos y la implementación de los mismos evoluciona a velocidad vertiginosa.

La problemática de la Seguridad

A lo largo de los últimos años los problemas de seguridad que se vienen observando en las empresas y organismos han sido una constante recurrente; se pueden diferenciar en tres grandes grupos:

Los problemas estructurales

Habitualmente la estructura de la organización no se hace pensando en la seguridad por lo que no hay una definición formal de las funciones ni responsabilidades relativas a seguridad.

No suelen existir canales de comunicación adecuados para tratar incidentes de seguridad, predominando los canales de tipo informal y el boca a boca.

Exceptuando determinados ambientes como la banca o la defensa, no suelen existir recursos específicos dedicados a seguridad, y cuando existen suelen dedicarse a la seguridad física (puertas, alarmas, dispositivos antincendios, etc.) por ser más fácilmente justificable su adquisición.

Problemas en el planteamiento

Los planteamientos de seguridad suelen adolecer de falta de coherencia ya que no suelen ser ni suelen están adaptados a las necesidades de la empresa.

Habitualmente las directrices no son homogéneas en toda la organización.

Como consecuencia de la falta de definición de funciones, nadie quiere responsabilizarse de los riesgos asumidos en la organización y nadie quiere adoptar medidas que puedan dificultar el proceso de negocio. El confusionismo operativo causa más estragos que legiones de hackers.

No se definen normas ni procedimientos salvo cuando su ausencia puede afectar al propio negocio (por ejemplo la existencia de copias de seguridad) o tras un incidente grave de seguridad. Buena parte de las medidas de seguridad actualmente implantadas, lo han sido como consecuencia de inconfesables incidentes: seguridad "a posteriori".

Al no existir beneficios inmediatos, resulta difícil justificar gastos y recursos.

El problema tecnológico

Quizá la tragedia a la que asistimos pueda compararse a la angustia de encontrarse en mitad de un incendio y no poder sofocarlo porque no sabemos usar el extintor que tenemos a nuestro alcance.

Existe tecnología suficiente. La más importante, la criptografía, se conoce y se usa desde épocas tan antiguas como el imperio romano (cifrado César). El sector de productos y servicios de seguridad crece y se fortalece a golpe de portada de periódico. A veces resulta difícil decidir qué producto elegir, de entre una importante oferta, para una determinada funcionalidad de seguridad (la actual batalla de las PKIs adquiere tintes dramáticos).

Pero la tecnología por sí sola no es la panacea: Las herramientas son un soporte, pero si no hay una base con ideas sólidas no solucionan los problemas.

Además, las herramientas existentes, de por sí, no cubren todas las necesidades. Una máxima que circula por internet: "un tonto con una herramienta, sigue siendo un tonto...pero peligroso". Uno de los principales problemas a que nos enfrentamos, no sólo en el sector de la seguridad, es la falta de personal "realmente" cualificado.

La sensación de falsa seguridad provocada por la excesiva confianza en las soluciones tecnológicas induce a bajar la guardia.

Resumiendo, la situación real suele ser que en las empresas y organismos el negocio y la imagen se anteponen a la seguridad. La organización crece e implementa soluciones de seguridad de acuerdo a necesidades puntuales, no hay definida una estrategia, ni normas ni procedimientos, es decir, lo habitual es que no se contemple expresamente la seguridad.

El problema principal que se desprende de todo lo anterior es que normalmente no se conoce el riesgo que se está asumiendo, ni se sabe cómo medirlo.

Planificando la Seguridad

Una vez identificados los problemas generales llega la pregunta que supone el principal escollo para desarrollar un plan que corrija la situación: ¿cómo se debe abordar la seguridad en la organización?

El Plan de Seguridad debe ser un proyecto que desarrolle los objetivos de seguridad a largo plazo de la organización, siguiendo el ciclo de vida completo desde la definición hasta la implementación y revisión.

La forma adecuada para plantear la planificación de la seguridad en una organización debe partir siempre de la definición de una política de seguridad que defina el QUÉ se quiere hacer en materia de seguridad en la organización para a partir de ella decidir mediante un adecuado plan de implantación (fruto de un Análisis de Riesgos previo) el CÓMO se alcanzarán en la practica los objetivos fijados.

La Política de Seguridad englobará pues los objetivos, conductas, normas y métodos de actuación y distribución de responsabilidades y actuará como documento de requisitos para la implementación de los mecanismos de seguridad. La política debe contemplar al menos la definición de funciones de seguridad, la realización de análisis de riesgos por cada sistema que soporta los procesos fundamentales del negocio, la definición de normativa y procedimientos, la definición de planes de contingencia ante desastres y la definición del plan de auditoría.

A partir del Análisis de Riesgos se podrá definir el Plan de Implementación, que es muy dependiente de las decisiones tomadas durante la fase de Gestión de Riesgos, en el que se contemplará: el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad.

Hay dos cuestiones fundamentales que deberán tenerse en cuenta para implantar con éxito una política de seguridad: Es necesario que la política sea aprobada para que este respaldada por la autoridad necesaria que asegure su cumplimiento y la asignación de recursos; y es necesario que se realicen revisiones periódicas que la mantengan siempre actualizada y acorde con la situación real del entorno.

Política de Seguridad, Plan de Seguridad, Análisis y Gestión de Riesgos y la implantación propiamente dicha están íntimamente relacionados ya que la implementación debe ser un fiel reflejo de los procedimientos y normas establecidos en la Política y Plan de Seguridad.

El Plan de Seguridad, exigencia legal recogida en el RD 994/1999 de 11 de Junio, para todos aquellos ficheros que contengan datos de carácter personal, debe estar revisado para adaptarse a las nuevas necesidades del entorno, los servicios que vayan apareciendo y a las aportaciones que usuarios, administradores, etc. Vayan proponiendo en función de su experiencia. La revisión es esencial para evitar la obsolescencia de la política debido al propio crecimiento y evolución de la organización. Los plazos de revisión deben estar

fijados y permitir además revisiones extraordinarias en función de determinados eventos (por ejemplo, incidentes).

La implementación debe ser auditado para asegurar la adecuación con las normas. Y debe realimentar a la Política de Seguridad. La experiencia, los problemas de implantación, las limitaciones y los avances tecnológicos, etc. permitirán que la política pueda adecuarse a la realidad, evitando la inoperancia por ser demasiado utópica y la mejora cuando el progreso lo permita.

Un enfoque como el propuesto asegurará la adecuación del nivel de seguridad implantado con las necesidades de la organización y el correcto seguimiento y control de los riesgos.

Criptografía, el brazo armado de la seguridad en internet.

La tecnología utilizada para mantener confidencialidad de datos y comunicaciones se llama criptología. Se trata aquí de operaciones matemáticas complejas, las cuales se aplican a los datos cuya confidencialidad se desea mantener. Criptología tiene dos componentes: Criptografía se refiere a las técnicas para convertir datos a una forma ilegible excepto por las personas autorizadas.

Criptanálisis se refiere a las técnicas que analizan los métodos de encriptación con el objetivo de encontrar una debilidad. Esos dos campos son íntimamente relacionados: un avance en las técnicas de criptanálisis motiva un avance en la criptografía y viceversa. Un método de criptanálisis efectivo se llama un ataque. Mucho del diseño de un sistema de seguridad se hace para defenderse contra uno u otro ataque conocido. Una problemática muy particular aquí se refiere a la
posibilidad de que los sistemas de seguridad diseñados hoy tendrán que resistir ataques no conocidos todavía, puesto que se descubrirán en el futuro.

La criptografía contemporánea comienza con el ya mítico artículo publicado por Diffie y Hellmann en 1977, donde se establecen las bases de la criptografía de clave pública. Desde principios de la década de los '90, el IETF y otras organizaciones públicas y privadas han desarrollado una intensa labor de estandarización que ha dado como resultado la aparición, alrededor de 1995 de productos comerciales que implementan el concepto de Infraestructuras de Clave Pública (PKI).

Una Infraestructura de Clave Pública es el conjunto de elementos Hardware y Software cuya misión es garantizar la implantación y la gestión de un entorno seguro para la identificación y autenticación de usuarios, basándose en el uso de Certificados Digitales y la generación para cada usuario de una pareja de claves, Publica y Secreta/Privada. La misión principal de una PKI es gestionar el ciclo de vida de los certificados digitales y de las claves asociadas.

Cada usuario dispone de un Certificado Digital, que contiene sus datos identificativos, y una pareja de claves relacionadas biunívocamente a través de un algoritmo matemático (RSA). La clave privada debe guardarla el usuario en algún soporte que puede ser, por ejemplo un PC o una tarjeta inteligente, según las necesidades propias de cada proyecto. La clave publica debe ser "publicada" para que sea conocida por el resto de los usuarios o aplicaciones con los que el usuario puede mantener una relación en la cuál es necesario garantizar la identidad.

Una PKI consta, básicamente de los siguientes elementos: Autoridad de Registro (RA), Autoridad de Certificación (CA), y un Servicio de Directorio para publicar los certificados y las claves públicas, aunque este último elemento suele ser independiente de la RA y CA, al menos comercialmente. También debe considerarse un elemento de esta infraestructura un Help Desk que atienda las incidencias.

Las principales funciones de una Autoridad de Registro (RA) son típicamente:

- Gestión de altas
- Generación de Claves, Publica y Secreta
- Almacenamiento en soporte personalizado de la Clave secreta
- Emisión de Certificados Digitales
- Almacenamiento en el Directorio del Certificado con su clave publica.
- Entrega personalizada del certificado al usuario.

El sistema de la RA debe estar aislado, sin comunicaciones exteriores y con vigilancia física. En buena medida la seguridad global del sistema depende de la seguridad de la RA.

Las principales funciones de una Autoridad de Certificación (CA) son típicamente:

- Firmar, con la clave secreta de la CA los Certificados emitidos por la RA.
- Gestión de los Certificados durante su vigencia.
- Comprobación de la lista de Certificados Revocados.
- Revocación de Certificados por caducidad, robo, pérdida, deterioro.

Estas infraestructuras son estratégicas, hoy en día, para cualquier negocio o proyecto basado en Internet, Intranet y Redes Privadas Virtuales, en definitiva para cualquier entorno de e-business. Por lo tanto, todas las grandes corporaciones, hoy en día están en proceso de evaluación e implantación de estas infraestructuras, con la complejidad que ello implica, no sólo desde el punto de vista técnico, sino sobretodo desde un punto de vista estratégico y de negocio, al afectar a todas las áreas de una compañía, incluso siendo válidas para dar servicio a un grupo de empresas.

La aplicación más popular hoy en día es la posibilidad de realizar la declaración del IRPF vía Internet. La Agencia Tributaria utiliza una PKI implantada por la Fabrica Nacional de Moneda y Timbre.

Retos de seguridad en el comercio electrónico.

El dinero electrónico

Durante los últimos años, la informatización de los bancos ha permitido que la mayor parte del dinero que circula por el mundo lo haga en forma de silenciosos bits, ristras de unos y ceros que viajan a través de líneas telefónicas o enlaces de satélite en lugar de hacerlo físicamente en forma de monedas y billetes.

Con el advenimiento de las tarjetas de plástico con banda magnética, fue posible que los usuarios accedieran a través de los cajeros automáticos a su dinero almacenado electrónicamente en el banco. Más aún, los cheques, las tarjetas de crédito y las de débito, permiten hoy en día realizar prácticamente cualquier tipo de pago en casi cualquier comercio y lugar del mundo. A medida que su uso se extendió y se venció la reluctancia inicial de los ciudadanos, fueron adoptados como medio de pago común en Internet y en situaciones en que las partes no se encontraban físicamente en contacto. Se utilizaron protocolos de comunicaciones ya existentes para salir del paso, como SSL, o se desarrollaron otros con el comercio electrónico en mente, como SET o CyberCash. Sin embargo, a pesar de su gran versatilidad y utilidad, el pago mediante tarjeta presenta el problema del elevado coste de una transacción, volviéndolas por tanto inadecuadas para compras de escaso valor.

Recientemente, están apareciendo en este escenario el dinero electrónico y las tarjetas monedero, con la posibilidad de abaratar los costes por transacción, haciendo posible el comercio de mercancías de escaso valor, tanto a través de Internet como en comercios en la calle. Tecnologías de dinero digital como eCash o MilliCent, permiten mover monedas electrónicas de un ordenador a otro, mientras que con el uso de tarjetas monedero o servicios como Virtu@lCash, se transfiere dinero de una cuenta a otra, incluso por importes muy pequeños.

A medida que las tarjetas monedero se popularicen, más y más bienes y servicios podrán ser pagados con ellas. Con el tiempo, y en la medida en que se acerquen a las prestaciones del dinero común en cuanto a facilidad de uso, rapidez, aceptación en comercios, anonimato y conveniencia, monedas y billetes tenderán a desaparecer en el futuro. El dinero digital debe poseer toda una serie de características presentes en las tradicionales monedas y billetes para que se convierta en medio de pago universal desplazando a estos últimos: seguridad, fiabilidad, escalabilidad, anonimato, aceptación, base de clientes, flexibilidad, eficacia, facilidad de integración con otras aplicaciones software y facilidad de uso.

Asumiendo la máxima de que "la economía es el motor del mundo", no es de extrañar que exista una gran variedad de protocolos ya en funcionamiento, otros en pruebas y aún más en fase de diseño. En estos momentos nos

encontramos en la excitante era del descubrimiento. Dentro de algunos años habrán sobrevivido los sistemas mejor adaptados a las necesidades del mundo real.

Cyberpunks

Inmediatamente conviene hacer la distinción entre el auténtico hacker, en su sentido original, que sabe programar en ensamblador y C, conoce los entresijos de Linux y Windows y sabe todo lo que se puede saber sobre protocolos TCP/IP, UDP e ICMP; y el conocido como "lamer", que tiene algunos conocimientos muy limitados de programación y mucho tiempo libre y aprovecha las vulnerabilidades descubiertas por los primeros en sistemas informáticos y los programas escritos por los primeros para explotar estos agujeros. Ser un auténtico hacker constituye un largo y arduo proceso de autoaprendizaje, mientras que para convertirse en "lamer" basta con frecuentar los conocidos sitios underground donde pueden obtenerse gratuitamente poderosas herramientas creadas por los verdaderos hackers.

En estas páginas de hackers, rara vez escritas por uno genuino, se ofrecen herramientas gratuitas de inusitada versatilidad y potencia, como las sofisticadas Nmap (www.nmap.org), Nessus (www.nessus.org) o Cheops (www.marko.net/cheops) para escaneo de puertos y detección de vulnerabilidades. El siguiente paso, una vez detectado con estos programas un buen agujero, consiste en intentar correr algún código que lo explote, códigos que normalmente se pueden encontrar en las mismas páginas de hacking (como por ejemplo www.anticode.com); o descargar un programa de ataque que ejecute un DoS (Denegación de Servicio) sobre la máquina objetivo para tirarla abajo; o probar con las instrucciones que se han encontrado en alguna buena página sobre cómo hacerse con privilegios de root explotando algún oscuro fallo de configuración en un servicio. Estos programas poseen un interfaz de usuario a veces sorprendentemente amigable y se encuentran a menudo incluso precompilados, por lo que el "lamer" ni siquiera necesita saber cómo compilarlos, no tiene más que ejecutarlos. Habida cuenta de la facilidad con que se obtienen, instalan y ejecutan estas herramientas, y dada la cantidad de información detallada acerca de agujeros, vulnerabilidades y caminos para explotarlas, resulta que prácticamente cualquiera con un ordenador y una conexión a Internet puede atacar con éxito una extraordinaria cantidad de sistemas en línea.

Estos ataques tienen éxito debido a que muchas redes funcionan ejecutando versiones antiguas de programas con vulnerabilidades conocidas y fácilmente explotables; configuraciones por defecto que dejan abiertas enormes puertas de entrada; contraseñas de fábrica que nadie se molesta en cambiar y que son de todos conocidas; servicios innecesarios que descubren multitud de puertos; y otras triquiñuelas que se describen con profusión de detalles en sitios underground. A la vista de la facilidad con que un niño puede convertirse en un hacker peligroso en unas pocas horas, no estaría de más que los administradores de sistemas y personal encargado de la seguridad informática se diesen una vuelta por las citadas páginas y utilicen las mismas armas que

los "lamers" para escanear sus redes, aprender acerca de los últimos exploits y tomar las medidas oportunas. Puede tratarse de una interesante y aleccionadora experiencia para más de uno, que siempre surtirá resultados positivos. Hoy en día, ser hacker resulta más sencillo que nunca. Dejar de ser una víctima fácil, también.

En algunos IRCs pueden leerse cosas como ésta:

"Yo no he pillado root ni he creado una cuenta, lo que pasa que desde esa shell de América, encontré el bouncer y para que no pillaran el host de la shell, porque era gratuito dos semanas y daban unos servicios que te cagas, que después iban a ser de pago, utilicé el bouncer ese que encontré".

Y en e-zines como la de los autobautizados "saqueadores", tras la descripción pormenorizada del ataque a los sistemas informáticos de una universidad y un e-banco, explotando vulnerabilidades de servidores Domino:

"CONCLUSIONES

¿Qué sería un estudio sin conclusiones?. La conclusión obvia es: 2 de 2.

Es disculpable que una universidad se deja la cartera encima de la mesa, no deberia ser la norma pero tampoco importa mucho. En cuanto al banco claramente se han preocupado algo mas por la seguridad pero como hemos visto no lo suficiente.

*No hagáis evaluaciones apresuradas, el problema no es que se pueda obtener esta información, el problema es **como** se obtiene. Con un navegador. Se podría disculpar si fuese necesario ser un 'gurú' de Domino para llegar a esto, lamentablemente a mi me basto dos días de leer guias para comenzar a encontrar huecos y sin ni siquiera usar o instalar Domino/Notes.*

No hace falta decir que algo falla, quizá todos estos programas son demasiados complejos para asegurarlos o puede que nadie este interesado en hacerlo.

Al final fueron necesarios cinco días de aprendizaje y un navegador, los administradores internos, la empresa de seguridad que (supongo) auditó el site y todos aquellos cuyo trabajo era prever este tipo de incidentes no debían disponer de tanto tiempo. O quizá no tienen ningún navegador.

Da que pensar.

Y recordad, hagáis lo que hágais.
Tened cuidado ahí fuera.

Paseante"

La mayoría de los ataques con éxito a ordenadores mediante Internet se pueden agrupar como la utilización de un reducido número de vulnerabilidades. La mayor parte de los ordenadores comprometidos durante el incidente conocido como "Solar Sunrise Pentagon" fueron atacados mediante una vulnerabilidad concreta. Una vulnerabilidad similar a esa fue la que se utilizó para controlar la mayor parte de los ordenadores que posteriormente se utilizaron masivamente en los ataques distribuidos de negación de servicio. De la misma forma, los recientes accesos ilegales a servidores web basados en Windows NT están asociados a la utilización de una vulnerabilidad sobradamente conocida. Otra vulnerabilidad, todavía, suficientemente estudiada para ser la causa de permitir el control ilegal de más de 30.000 sistemas Linux.

Con sólo algunas vulnerabilidades, en definitiva, se realizan la mayor parte de los ataques con éxito debido, en gran parte a que los atacantes son oportunistas – utilizan la vía más fácil y conveniente. Utilizan las brechas mejor conocidas mediante el uso de diversas herramientas de ataques muy efectivas y ampliamente difundidas. Se aprovechan de aquellas organizaciones que no aplican los parches para resolver los problemas, realizando habitualmente ataques de forma indiscriminada, rastreando en Internet por la existencia de sistemas vulnerables.

La mayor parte de los administradores de sistemas afirman que no han solucionado estas brechas de seguridad por la simple razón que desconocen cuales de los 500 problemas potenciales son los más peligrosos y carecen del tiempo necesario para poder corregirlos todos.

La comunidad de profesionales de la seguridad informática desea resolver este problema identificando las áreas de seguridad en Internet más críticas – el grupo de vulnerabilidades que los administradores de sistemas deben eliminar de forma inmediata. Esta lista consensuada, a la que denominaremos Top Ten, es un ejemplo sin precedentes de cooperación activa entre la industria, los organismos públicos y las instituciones educativas. Los participantes provienen de las agencias federales con mayor conciencia en temas de seguridad, de los principales distribuidores de productos de seguridad, de consultoras especializadas; de diversas universidades con programas especializados en seguridad y del CERT/CC y el SANS Institute. Al final del articulo incluimos la relación completa de participantes.

Esta es la lista de los 10 problemas de seguridad en Internet más frecuentemente utilizados, con la relación de acciones que deben tomarse para proteger los sistemas de las mismas.

1. Debilidades de BIND: nxt, qinv e in.named permiten comprometer la cuenta de root inmediatamente.

2. Programas CGI y extensiones de aplicación (por ejemplo, ColdFusion) instalados en servidores web.

3. Debilidades en llamadas de procedimiento remoto (RPC) en rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager) y rpc.statd que permiten la obtención inmediata de privilegio de root.

4. Agujero de seguridad RDS en Microsoft Internet Information Server (IIS).

5. Debilidad por desbordamiento de buffer en sendmail; ataques mediante áreas de interconexión de memoria y MIMEbo; todas ellas permiten comprometer la cuenta de root inmediatamente.

6. sadmind y mountd.

7. Compartición de archivos global y compartición de información inapropiada mediante NetBIOS y los puertos 135 -> 139 en Windows NT (445 en Windows 2000), exports de NFS en Unix (puerto 2049), compartición vía web en Macintosh y Appleshare/IP en puertos 80, 427 y 548.

8. Cuentas de usuario, especialmente la de root o administrador, sin contraseña o con contraseña poco segura.

9. Vulnerabilidades de desbordamiento de buffer o configuración incorrecta en IMAP y POP3.

10. Nombres de comunidad SNMP por omisión ('public' y 'private').

Los medios de pago

El 23 de marzo, fueron arrestados por la policía británica dos personas, (la prensa británica los califica como "hackers", ambos de 18 años de edad, y ambos galeses) por la entrada ilegal en 9 webs de e-commerce, de cinco países diferentes, (Inglaterra,USA, Canadá, Tailandia, y Japón) apropiándose de la información de 26.000 tarjetas de crédito.

Se les acusa de violar la "Computer Misuse Act" de Reino Unido de 1990. Las webs afectadas han comunicado que los adolescentes habían usado un agujero en la seguridad de SQL Server de Microsoft, aunque en la web de feelgoodfalls.com, se entró a través del agujero del programa Microsoft Storefront. Según algunos de los afectados, también habría que achacar el resultado final a la mala organización de las propias empresas, la mayoría de ellas pequeñas empresas.

Según el FBI comenzaron a actuar en Enero, y usaban el nombre de "curador" en sus ataques, que no sólo quedaban en eso, sino que después publicaban los números de las tarjetas en las webs: e-crackerce.com y free-creditcard.com, así como en la página personal de xoom.com. Esta última fue cerrada en febrero, y actualmente lo están también las otras dos. En ellas había mensajes como "Gracias a mi amigo Bill Gates, alguien que vende productos como SQL Server, no puede ser tan malo".

Según el FBI el incremento de este tipo de incidentes empieza a ser alarmante, si bien es cierto que la suplantación de personalidad o el "robo de identidad" no es nada inventado en este siglo, si es cierto que la seguridad en las transacciones es una de las asignaturas pendientes de Internet.

Según las autoridades americanas, se han publicado las estadísticas correspondientes a 1999, y tan sólo en la "Social Security Administration" (es decir, el organismo que rige la Seguridad Social norteamericana) se han recibido mas de 30.000 quejas sobre mal uso de los números de las tarjetas de seguridad social, la mayoría sobre "robo de identidad", o suplantación de personalidad. Y ello frente a las 11.000 de 1998, o las 7.868 de 1997. Es decir, aumentó casi el triple el número de incidencias en un año.

El número de la Seguridad Social en Estados Unidos se usa como el número de carnet de identidad en otros países, así pues basta tener el número de la tarjeta de crédito y el número de la Seguridad Social de la persona para "poder hacer compras on-line" en la mayoría de los casos. Es más, hay empresas que por 49 dólares ofrecen ese número a quien lo solicite, o empresas, como Net Detective 2000, que se promociona con anuncios como "la increíble herramienta que te permite saber TODO lo que querías sobre tus amigos, familia, vecinos, empleados o tu jefe". Y son legales.

El Instituto para la Seguridad Informática (Computer Security Institute) ha publicado su encuesta "delito informático y seguridad 2000", basándose en la respuesta de 643 directivos de empresas, gobierno, instituciones financieras, hospitales y Universidades. El FBI ayudó en la encuesta, y muestra que 273 encuestados declaran perdidas económicas, robo de información y fraude financiero. El 90 por ciento declaran haber tenido problemas de seguridad, el 71 por ciento en relación con accesos no autorizados

En ocasiones, el hacker no necesita desarrollar especiales dotes y maestría para perpetrar sus ataques, sino que se limita a explotar el descuido, el desconocimiento o las prisas de un presionado administrador del sistema.

Cuando se decide emplear un software comercial para montar un comercio electrónico, una tienda en Internet, hay que leer muy bien todas las instrucciones de instalación y proceder a una instalación cuidadosa, y prestar atención a las partes más importantes del programa. Incluso en ocasiones hay que llegar más allá de la propia documentación y comprobar personalmente todos los elementos que conforman el comercio, como si de una tienda real se tratara y pusiéramos lejos del alcance de los clientes la caja registradora. La base de datos de productos, de usuarios y de pedidos son datos fundamentales que deben estar
cuidadosamente protegidos

Por otro lado la "industria" de las tarjetas de crédito rechaza esta visión pesimista y afirma que si bien el fraude existe, no es más que un pequeño porcentaje de los cientos de billones de dólares que las compras con tarjeta de crédito mueven cada año. Sin embargo, el pasado 3 de Noviembre, Visa Internacional ha reconocido estar preparando un plan de choque contra las

tiendas virtuales clientes que no garanticen unas mínimas medidas de seguridad para las transacciones electrónicas.

Dispuesta a disipar los miedos del usuario hacia el comercio on-line, VISA ha anunciado un plan mediante el que se cumplimentará por la razón y por la fuerza lo que los cyberpunks no han logrado mediante sus continuas incursiones en webs comerciales: proteger los números de tarjeta y datos de sus clientes.

Bajo este plan, el gigante de medios de pago californiano comenzará a monitorizar los miles de negocios on-line que aceptan transacciones con tarjeta Visa para garantizar el cumplimiento de la normativa de seguridad de la compañía. Esta normativa recomienda el uso de cortafuegos, criptografía y la actualización contínua del software de base añadiendo los necesarios parches de seguridad. Habrá sanciones económicas para aquellos negocios que no cumplan los estándares.

Supongamos que un supuesto cracker ha conseguido un número blanco de tarjeta de crédito, en alguno de los webs mencionados arriba. Veamos con un ejemplo cómo podría explotarlo, según un reciente artículo en un popular informativo on-line:

1. Un usuario (la víctima) entra en un sitio de mercadillo o subastas "online", donde puede observar una auténtica ganga por un precio muy inferior al del mercado, con manuales, embalajes originales, etc.

2. El usuario se muestra interesado por semejante oferta y se pone en contacto con el propietario.

3. El propietario (nuestro supuesto cracker) le dé todas las facilidades del mundo. Incluso se ofrece a enviar la mercancía al domicilio del incauto cliente, sin una señal monetaria previa. Sí lo exige un compromiso de devolución del producto, si no se está satisfecho, o la transferencia de la cantidad acordada si la mercancía le satisface.

4. Dado semejante "chollo", el cliente no duda en proporcionar su dirección postal, nombre, etc.

5. Con esa información, el "pretendido" propietario de la mercancía realiza una compra on-line del producto en cuestión, naturalmente a precios de mercado. Para ello emplea una tarjeta de crédito robada. Como dirección de envío, pone los datos del usuario inicial.

6. Tras unos días, el usuario recibe la mercancía en su casa y, con casi total seguridad, realizará la transferencia bancaria.

La historia termina con que al propietario de la tarjeta de crédito se le efectúa al cargo, el usuario final tendrá en su propiedad mercancía robada y el verdadero criminal recibirá un jugoso ingreso en una cuenta de difícil seguimiento, típicamente en el extranjero.

La seguridad total no existe. Es un mito. Siempre existirá un riesgo residual que necesita ser transferido. La verdad es que es muy difícil, incluso para las páginas con las defensas más fuertes, asegurar que sus páginas Web no serán hackeadas, aunque siempre pueden asegurar una parte de sus pérdidas causadas por estas intrusiones. Tampoco debemos olvidarnos del "factor humano", o como diría Donn B. Parker, padre de los ciberpolicías norteamericanos del Standford Research Institute: "Insiders take billions".

Con todo esto, no es de extrañar que algunas compañías de seguros, que muchas veces se han considerado con poco atractivo para internet, están siendo más usadas como consecuencia de los últimos ataques malintencionados sufridos por algunas páginas famosas. omo el portal Yahoo!, donde ya están asegurados por si se quedan sin servicio a causa de un fallo eléctrico o un terremoto. Pero las compañías de seguros aún balbucean y dudan ante un eventual desembarco en este nuevo negocio.

Problemas de procedimientos

La entrega de pedidos es el punto débil del e-commerce en Europa Según un estudio realizado por Andersen Consulting mediante 445 compras efectuadas en 162 webs de Alemania, España, Francia, Italia, Reino Unido y Suecia, existen serios problemas en la entrega de los pedidos, ya que, en muchos casos, es necesario esperar varias semanas antes de recibir lo comprado, o incluso no recibirlo nunca.

El 39% de las compras on-line no pudieron concluirse por cuestiones técnicas o de procedimiento. El 57% de los pedidos realizados se entregaron en un plazo de siete días, y el 60% de los pedidos internacionales han tardado más de una semana.

En los casos en que no se ha proporcionado una fecha de entrega, el 59% de las veces no se entregó el pedido.

La democratización del e-business: PSAs

PSA representa la tendencia más novedosa en modelos de negocio basados en Internet. Se fundamenta en ofrecer una solución de red integrada y total, que incluya software, hardware, cableado, mantenimiento, soporte, conectividad a Internet con acceso fijo y/o móvil (WAP), actualización constante tanto de los programas como del hardware y otros servicios igualmente interesante. Básicamente, se trata de servir en alquiler software especialmente caro, personal
cualificado, servidores y canales de acceso de gran capacidad, de manera que la empresa que contrata al PSA se evite esas inversiones iniciales, que de entrada pueden resultar prohibitivas. La idea consiste pues en alquilar en vez de comprar, externalizar en vez de afrontar grandes gastos.

Desplegar una sofisticada aplicación de comercio electrónico, con la consiguiente inversión en programas y servidores, mano de obra, mantenimiento, etc., pasaría a ser una posibilidad asequible con PSA, al alcance de pequeños empresarios de limitados recursos de Tecnologías de la Información. La PSA hace frente a las necesidades de adquirir servidores más potentes o canales de comunicación de mayor capacidad.

Pero no todo pueden ser ventajas. Su riesgo más evidente es para la seguridad de la empresa que contrata al Proveedor de Servicios de Aplicaciones. Cuanto mayor sea el atractivo de hacerse con la información mantenida por el PSA, mayor será el número de ataques. Resulta obvio que de forma natural los PSA se convertirán en blanco preferido de los hackers.

Los servicios de seguridad mínimos exigibles al PSA serán:

- Cifrado de las comunicaciones, utilizando canales seguros con SSL de 128 bits o acudiendo a tecnologías de VPN (cuidado aquí con soluciones cerradas como PPTP de Microsoft, con agujeros ya encontrados).

- Autenticación fuerte, basada en técnicas criptográficas robustas e infalsificables, que por supuesto deberán guardar proporción con el nivel de sensibilidad de la información a proteger.

- Detección de intrusos, escaneos de puertos y de otras operaciones sospechosas.

- Se deberá dotar al sistema de una capacidad de respuesta rápida y eficaz.

- Utilización de un sistema operativo seguro, o al menos, seguramente configurado, con definición de permisos de accesos muy restrictivos y especial cuidado en programas ejecutables accesibles a través de las redes. Resulta fundamental que los clientes de un PSA no puedan acceder a los datos de otros clientes (de la competencia) albergados en el mismo PSA.

- Mantenimiento realizado preferiblemente desde las propias consolas de los servidores, ya que se previenen problemas de agujeros en los accesos remotos. Es importante establecer quién accede a los datos de quién. ¿Puede un administrador del PSA acceder rutinariamente a la información confidencial y sensible de una empresa?

A pesar de todas las medidas de seguridad, los mayores peligros a los que se enfrenta un servicio de PSA ofrecido a través de redes públicas son:

- Denegación de servicio: si el PSA deja de prestar el servicio transitoriamente, bien por ataques de hackers, bien por causas técnicas, la empresa puede ver su negocio seriamente afectado, dependiendo su impacto de la mayor o menor necesidad de prestación continuada del servicio a sus clientes. Hoy por hoy, habida cuenta del ciclo de vida tradicional del software, donde son los clientes, y no sus creadores, los que

prueban el software y descubren vulnerabilidades, resulta muy arriesgado confiar en que el PSA se mantendrá a prueba de ataques con todas las brechas de seguridad cerradas y que garantizará un servicio durante el 100% del tiempo, incluso bajo ataques con éxito. La redundancia física y lógica de servidores juega aquí un papel crítico.

- El personal interno: una vez más, el mayor riesgo no procede de fuera, sino de dentro del propio PSA. Si alberga en él información confidencial de gran valor, un empleado desleal del PSA o implantado allí por un rival podría sentirse tentado de robarla para su uso o venderla al mejor postor. Nadie como él conoce cómo funciona internamente el Proveedor, por lo que nadie mejor que él para atacar sin dejar rastro. Estos empleados también podrían ser vulnerables a ataques de ingeniería social, sobornos, extorsiones, etc.

En la actualidad, los PSA se encuentran en su infancia. A pesar de la publicidad, los riesgos superan con mucho a las ventajas como para apostar fuerte por un PSA de acceso a través de redes públicas. Por supuesto, esta situación cambiará en el futuro, especialmente en la medida en que la seguridad se afronte como un objetivo prioritario del ASP y no como una mera cláusula del contrato

La Firma Electrónica y su validez jurídica

La firma electrónica, como ya se sabe, se reguló en España con el Real Decreto Ley 14/99 de 17 de septiembre, se intentaba con ello aumentar la seguridad y confianza en las comunicaciones telemáticas, además de garantizar la autenticación y la identidad del comunicante. Intentando cumplir las siguientes funciones, así identificación y atribución del mensaje (indica el origen y voluntad del firmante), función de privacidad (cifrado de mensaje y firmante), función de seguridad e integridad (evidencia si ha habido apertura o alteración del mensaje).

Cuando salió la ley, hay que reconocerle que fue una de las primeras sobre dicho tema. Se conocían sólo la Ley Alemana, la de Singapur, y la del estado de California (USA), pero esa celeridad ha sido criticada por algunos ya que, según éstos, ha dejado algunas lagunas sin resolver, como luego veremos, que pueden hacer de la seguridad una simple ilusión.

La ley maneja diferentes conceptos, así la "firma electrónica" (conjunto de datos, mensaje e identifica al autor o autores), y "firma electrónica avanzada" o digital (permite la identificación de signatario, le vincula, y detecta modificaciones del mensaje, en su caso).

La firma electrónica avanzada tiene en relación con el documento electrónico, el mismo valor jurídico que la firma manuscrita en relación con el documento en formato papel. La firma electrónica avanzada será admitida como prueba en juicio respecto a los datos signados, y será valorada conforme a los criterios de apreciación judicial establecidos en las normas procesales. El documento

firmado electrónicamente no tiene valor de documento público: la firma electrónica no sustituye la función del fedatario público en relación con la formalización, validez y eficacia de las obligaciones y los contratos. Y esto es importante distinguirlo, la firma electrónica no hace de Notario nunca, tendrá valor de documento privado, (es decir, menor fuerza probatoria en un juicio que el documento público).

Y además para que esto sea así, es decir, si deseamos que la firma electrónica sea equivalente a la firma manuscrita en un juicio ("firma avanzada"), los certificados que se empleen en la comprobación de una firma electrónica deben haber sido expedidos por un proveedor de servicios de certificación (PSC) acreditado en España que cumpla con la normativa del RD-L 14/99 y con todos los requisitos legales necesarios para ser un PSC, obviamente.

La prueba de la compra es la clave para dotar al comercio electrónico de seguridad jurídica. Esta seguridad jurídica por el momento solo es alcanzable con la firma electrónica, bien sea a través de las Infraestructuras de Clave Pública y la firma digital o con la utilización de otra técnica de firma electrónica en donde necesariamente intervenga una tercera parte de confianza o Trusted Third Party, que certifique que los datos de firma consignados en el documento de compra pertenecen a una determinada persona.

El problema fundamental radica en la valoración que de esta prueba realicen los tribunales de justicia. A pesar de que el RDL 14/1999 de 17 de septiembre otorga a la Firma Electrónica el mismo valor jurídico que a la Firma Manuscrita, el valor probatorio en juicio es distinto. Generalmente en un proceso judicial la prueba pericial caligráfica suele ser prueba plena, mientras que la prueba de una firma electrónica es una prueba de presunciones. Esta diferencia estriba en el rasgo o peculiaridad física que tiene la firma manuscrita, ya que la misma ha de ser realizada por la mano de la persona que firma, mientras que la firma electrónica es la introducción de una clave secreta o PIN para la ejecución de la misma en el documento electrónico, de ahí que se presuma que la ha realizado esta persona, pero puede ser probable que otra persona que se conozca el PIN o clave secreta haya ejecutado esa firma. En este sentido, se alcanzará igual valor probatorio entre ambos tipos de firma cuando en la ejecución de la firma electrónica intervengan rasgos biométricos de la persona, es decir, cuando sea el iris del ojo, la huella dactilar etc. el rasgo físico que ejecute la firma almacenada en el ordenador o en la tarjeta chip, solo entonces podrá existir igual efecto probatorio en juicio, y eso a pesar de que en nuestro ordenamiento jurídico existe la libre valoración de la prueba por parte de los jueces y tribunales, y por tanto al final la última palabra la tiene el juez. Habrá por tanto, que esperar a que se establezca este sistema biométrico para conseguir plena equiparación en juicio con la firma manuscrita.

Mientras tanto tendremos una prueba de presunciones que también será válida para probar que una determinada oferta fue aceptada.

Hasta el momento la técnica más segura sería la combinación de los certificados de firma X509 v3 almacenados en tarjeta chip, y el protocolo de comunicación seguro SSL.

A pesar de la seguridad en la comunicación, la utilización este protocolo de comunicación en el pago de los productos y servicios podría producir desconfianza en el Cliente, ya que potencialmente el Vendedor puede realizar cualquier tipo de fraude con total impunidad al poseer su número de tarjeta y no quedar garantizada la integridad del documento de pago. Sólo las empresas con muy buena reputación podrían, a priori, contar con la confianza del consumidor. Por otro lado, el consumidor en el caso de pago con tarjeta puede negar la compra del producto y el banco estará obligado a devolver el dinero si "no ha sido presentada directamente o identificada electrónicamente" (artículo 46 Pago mediante tarjeta de crédito, del capítulo II Venta a distancia, del título III Ventas especiales de la Ley del comercio minorista L7/96 de 15 de Enero). Aquí no habría muchos problemas si lo comprado es un bien físico y hay una dirección de entrega, pues podríamos saber de quién se trata, el problema surge cuando se utilizase para comprar bienes o servicios intangibles, es decir, bienes que no necesitan traslado físico, ya que sería más difícil de probar a donde ha ido a parar el producto o servicio y por tanto si se comete el fraude el perjudicado es sin duda alguna el comercio. Además, el más que posible fraude con números de tarjetas robados hace que las Entidades de Crédito añadan una comisión en las compras bastante elevada (un 5% +/-) para compensar este tipo de fraude. Esto hace que el precio de la compra se incremente considerablemente, lo que anula el atractivo inicial de comprar por Internet: los precios bajos.

Si embargo, con la emisión de Certificados para firma se producirá una mayor confianza tanto en el consumidor como en el vendedor. Esto es debido a que al firmar el pago o formulario de pedido hay integridad del documento (es decir el vendedor no puede cambiar la fecha o cualquier otro dato), hay autenticidad en la compra (el comprador es quién dice ser pues su firma digital lo prueba, ya que está respaldada por una tercera parte de confianza o autoridad de certificación) y se produce el efecto del no repudio. De este modo con la combinación de estas dos técnicas de seguridad se podría establecer un comercio electrónico seguro para las tres partes intervinientes, Consumidor Vendedor y Banco. Con esta técnica habría todavía un problema a salvar, y no es otro que la intimidad de los datos de la tarjeta, los cuales no quedarían asegurados, siendo imprescindible utilizar otra técnica más segura SET (Secure Electronic Transaction) que por el momento no ha visto su despegue definitivo.

RIESGOS DE RESPONSABILIDAD CIVIL EN INTERNET .

AGERS 2.000

Gonzalo Iturmendi Morales.
Abogado.

Fuentes de riesgos de responsabilidad civil de Internet

Internet ha dejado de ser un simple sistema de transmisión para pasar a un sistema de negocios y de comunicación social.[1]

Juan Luis Cebrián afirmaba en una conferencia pronunciada en Bruselas a finales del año 1997 que "las nuevas tecnologías cambiarán la naturaleza del poder".. En la sociedad de la información la capacidad de control de los Gobiernos es muy inferior al de algunas grandes empresas como las de Bill Gates: el sistema Windows está implantado en el 80% de los ordenadores del mundo.

Una simple enumeración de posibles conflictos y manifestaciones de riesgos de responsabilidad civil en Internet [2] puede causar auténticos escalofríos, de ahí que se imponga su sistematización en conjuntos.

---

[1] Hay actualmente en el panorama editorial español varias obras que permiten al profesional interesado situarse en la nueva forma de entenderlos negocios y, en general, la visa en sociedad, que suponen las nuevas tecnologías de la información.

- López Garrido, D.: La sociedad informatizada y la crisis del Estado de bienestar. Revista de Estudios Políticos (REP), núm. 48, Nov.-Dic. 1985, 27

- Bustamante Donas, J.: ¿Sociedad informatizada, sociedad deshumanizada? Gaia, Madrid, 1998

[2] Por ejemplo, entre la muchas manifestaciones y problemas de responsabilidad civil en Internet encontramos:
1.- Responsabilidad civil profesional por errores y omisiones.
2.- Fraude informático.
3.- Abusos de E.MAIL. Por ejemplo: campañas de desprestigio, de marginación de productos o empresas, complots, etc...
4.- Virus informáticos. A) Accidentales. B) intencionados.
5.- Copyright.
6.- Pornografía.
7.- Fallos del sistema que provocan pérdidas.

Hay tres grandes grupos de problemas de seguridad. El primero tiene que ver con los actos malintencionados y la necesidad de proteger la información que fluye a través de la red. El segundo está relacionado con la intimidad de las personas y otros derechos fundamentales como la libertad de expresión, la privacidad, el honor, la propia imagen y el secreto de las comunicaciones. Y en tercer lugar todo lo relacionado con la seguridad de la contratación electrónica. Si bien es cierto que el primero y el tercero pueden resolverse –dado su carácter tecnológico- y con el tiempo dispondremos de medidas de prevención que minimicen estos riesgos, sin embargo, sin embargo el problema segundo es social al ser la red un sistema de comunicación social.

A nuevas tecnologías nuevos riesgos emergentes y de entre ellos destacan los que ahora nos ocupan, los relativos a las distintas manifestaciones de la responsabilidad civil en Internet , pues si bien es cierto que las nuevas tecnologías ayudan al desarrollo, no es menos cierto que su aparición en la sociedad genera un sinfín de riesgos de responsabilidad civil cuya primera máscara a simple vista puede atemorizar por la novedad y sofisticación técnica del medio virtual donde se manifiestan. Sin embargo un estudio detallado de estos nuevos riesgos emergentes de responsabilidad civil nos permitirá ubicarlos en el justo marco que les corresponde, mediante el necesario retorno a los fundamentos y principios básicos de la responsabilidad civil que nos posibilite abordar la selva mediática sin complejos y en el convencimiento de que estos fenómenos novedosos son perfectamente susceptibles de sistematización y estudio.

La globalización comunicacional conlleva cambios tecnológicos vertiginosos que encuentran su principal campo de operaciones en Internet . En todo caso, los beneficios van a ser superiores a los riesgos si afrontamos los desafíos con un cambio de mentalidad. .

8.- Intimidad. Acceso a datos de carácter personal. Acceso a correo sin autorización. Grabaciones sin consentimiento de ficheros, sonido, imagen, etc.
9. – Honor. Informaciones. Propaganda. Publicidad. Opiniones.
10.- Imagen. Utilización indebida. Derechos de propiedad intelectual. Derechos de imagen.
11.- Chateo.
12.- Acceso no autorizado a datos de terceros.
13.- Comercio electrónico e incumplimientos contractuales.
14.- Infidelidad de empleados.
15.- Delitos informáticos.
16.- Terrorismo cibernético.

Los especialistas coinciden en afirmar que Internet adquirirá la máxima relevancia en las aplicaciones de negocio y tendrá una influencia menor en el entretenimiento. El impacto será grande en el ámbito de las comunicaciones móviles, en el control de dispositivos y aparatos domésticos y en el de la automatización industrial.

La capitalización total del mercado de ordenadores es aproximadamente de seis billones de dólares, mientras que el de las empresas de Internet es ahora de un billón. Quizá Internet esté metido en una burbuja bursátil, pero los mismos que creen en ella esperan que el mercado de Internet se multiplique, por lo menos, por seis.

Si se pretende que Internet contribuya a reducir desigualdades no va a faltar trabajo. Un sondeo de PricewaterhouseCoopers entre un millar de ejecutivos concluye que la red está ampliando el abismo que separa los países ricos de los pobres. Aún hay 2.000 millones de seres humanos, un tercio de la población mundial, que nunca ha usado el teléfono.

Nos proponemos la tarea de diseñar un pequeño mapa que permita "navegar" por la vorágine de las distintas fuentes de responsabilidad civil de Internet . Para ello nos ayudaremos de los tres ejes disponibles al alcance de cualquier investigador que desee iniciarse o bien profundizar en la materia que nos ocupa: las normas vigentes, la doctrina científica y las todavía escasas resoluciones judiciales pronunciadas sobre estos conflictos.

I

La seguridad en Internet . Hechos malintencionados, delitos informáticos, fraude, hackers y virus informáticos.-[3]

Encontramos un primer núcleo de fuentes de responsabilidad civil en las derivadas de la comisión de delitos y faltas.

La responsabilidad puede derivarse de actos ilícitos tipificados en la ley penal, que lleven aparejada la obligación de resarcimiento al perjudicado como consecuencia de la comisión del delito o falta, tal es el caso de la responsabilidad civil por ilícito penal.[4]

Una cosa es la responsabilidad criminal, imputable a quienes realizan actos voluntarios subsumibles en las leyes penales, y otra bien distinta la obligación civil de reparar daños que, aunque tengan su origen remoto en los mismos hechos que la ley declara punibles, se rigen por disciplina diferente y están sometidos al conocimiento de la jurisdicción civil.

Es doctrina reiterada de la Sala Segunda del Tribunal Supremo que la jurisdicción penal es soberana para declarar la procedencia de la indemnización de daños y perjuicios, sin más límites que las siguientes:

a) Que consten los datos fácticos indispensables para poder determinar los perjuicios o daños, de modo que las bases, no su cuantía, es lo que queda sujeto a la revisión.

b) Que la antedicha libertad de cuantía queda tan solo limitada, por las cantidades que se fijen por las acusaciones públicas y privada cuando ejercitan la acción civil derivada de la penal.

---

[3] El pensamiento jurídico y económico se han venido ocupando desde hace ya varios años del gravísimo peligro que, para la economía y el orden político de una sociedad, suponen los delitos informáticos. A este respecto, pueden consultarse:

- Gutiérrez Francés M.L. Fraude Informático y Estafa, Ministerio de Justicia, Madrid, . 1991.
- Settembrino, F.:¡Ya ha llegado el nuevo *cookie*!, Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XV, nº 65, primer trimestre de 1999

[4] Responsabilidad criminal o delictual, que lleva aparejada la responsabilidad civil accesoria (Artículos 1902 del Código civil, 116 al 122, y 125 del Código penal).

Podemos distinguir en el nuevo Código Penal dos grandes grupos de delitos cometidos con la intervención de la Informática: por una parte, los delitos contra la intimidad [5], y por otra, los delitos contra el patrimonio y el orden socioeconómico[6].

[5] **-Delitos informáticos contra la intimidad.-**

Artículo 197.-

1. 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.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3. Se impondrá la pena de prisión de dos a cinco años si se difunde, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta tipificada en el párrafo anterior.

4.Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 y 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Artículo 198.-

La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

Lo dispuesto en los dos artículos anteriores será aplicable también al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes (art. 200 del Código Penal).

[6] **Delitos informáticos contra el patrimonio y el orden socioeconómico.-**

Robo con fuerza en las cosas.-

El Código Penal tipifica en el artículo 239 como robo con fuerza en las cosas el uso de tarjetas magnéticas o perforadas perdidas u obtenidas por un medio que constituya infracción penal. De acuerdo con la normativa comunitaria cabe afirmar la exoneración de responsabilidad del titular de tarjeta sustraída por los cargos realizados con posterioridad a la denuncia del hecho de la sustracción y la limitación de su responsabilidad a 150 euros por las disposiciones anteriores a la denuncia. En el supuesto, más que difícil, de que se encuentre al autor de la sustracción y se le condene por este delito, será éste el responsable de la reparación de los perjuicios económicos causados.

Estafa.-

El artículo 248.2 del Código Penal dispone que:

> "También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante, consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero."

Con arreglo al estricto concepto de estafa establecido en el número 1 del mismo precepto, estas conductas quedarían impunes por ausencia del requisito del engaño, por cuanto no puede ser destinatario del mismo una máquina. El requisito del engaño es sustituido por el de manipulación informática o artificio suficiente. Se recoge por tanto, una expresión de gran amplitud que permite encuadrar todos los supuestos de manipulación informática que produzcan una transferencia patrimonial no consentida en perjuicio de tercero.

Daños.-

El artículo 264.2 del Código Penal establece:

> "La misma pena (prisión de uno a tres años y multa de doce a veinticuatro meses) se impondrá 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."

Propiedad intelectual.-

El Código Penal dentro del Título XIII, dedicado a los delitos contra el patrimonio y contra el orden socioeconómico, regula en el Capítulo XI los delitos relativos a la propiedad intelectual e industrial, al mercado y a los consumidores.

En los artículos 270 a 272 el Código Penal recoge la protección penal que nuestro ordenamiento jurídico da a la propiedad intelectual. El Texto Refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo, de 12 de Abril de 1.996, define el objeto de la propiedad intelectual en su artículo 10:

> "Son objeto de propiedad intelectual todas las creaciones originales literarias, artísticas o científicas expresadas por cualquier medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro.'

Y a continuación dicho artículo enumera una serie de creaciones susceptibles de constituir propiedad intelectual citando entre ellas expresamente los programas de ordenador.

El artículo 270 del Código Penal por un lado ampara el derecho a la producción y creación literaria, artística, científica y técnica contra los plagios y la reproducción, distribución o comunicación inconsentida; y por otro lado, ampara el derecho de explotación exclusiva y el control de las creaciones, obras y programas informáticos de los autores o asimilados.

Artículo 270.-

Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte o comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización.

Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

El artículo 271 del Código Penal recoge dos subtipos agravados que se refieren a cualquiera de las conductas castigadas en el artículo 270, cuando concurra alguna de las siguientes circunstancias:

a) Que el beneficio obtenido posea especial trascendencia económica.

b) Que el daño causado revista especial gravedad.

La responsabilidad civil derivada de los delitos relativos a la propiedad intelectual se regirá por las disposiciones de la Ley de Propiedad Intelectual. El Código Penal remite por tanto, a los artículos 133 a 135 del Texto Refundido de la Ley de Propiedad Intelectual, aprobado por Real Decreto Legislativo, de 12 de Abril de 1.996.

El artículo 133 otorga acciones al perjudicado, tanto para exigir el cese de la actividad ilícita, como la indemnización por daños y perjuicios. El artículo 134 determina los distintos grados y formas del cese de la actividad ilícita. Y el artículo 135 dispone que la acción para reclamar prescribe a los cinco años desde que el legitimado puede ejercitarla.

Propiedad industrial.-

El Código Penal ampara el derecho exclusivo que la patente o el modelo de utilidad confieren a su concesionario. El artículo 273 sanciona las conductas de los que con fines industriales o comerciales, sin consentimiento del titular de una patente o modelo de utilidad y con conocimiento de su registro, fabriquen, importen, posean, utilicen, ofrezcan o introduzcan en el comercio objetos amparados por tales derechos. Asimismo sanciona a los que de igual manera, y para los citados fines, utilicen u ofrezcan la utilización de un procedimiento objeto de una patente, o posean, ofrezcan, introduzcan en el comercio, o utilicen el producto directamente obtenido por el procedimiento patentado. En el apartado 3º de este artículo se hace una referencia especial a los modelos o dibujos industriales o artísticos o topografías de productos semiconductores.

- Espionaje industrial.-

Son los artículos 278 a 280 del Código Penal, bajo el epígrafe de delitos relativos al mercado y a los consumidores los que tipifican el espionaje industrial.

Aparte de estos dos grupos de delitos en los que se hace una referencia expresa en el nuevo Código Penal al medio informático, no cabe duda de que también se pueden cometer otros delitos utilizando para ello la informática. No hay que olvidar que la informática es un instrumento o herramienta con que se pueden hacer muchas cosas tanto lícitas como ilícitas.

Según un estudio de la Comisión Federal de Comercio de Estados Unidos la mayoría de las conductas delictivas de fraude en el comercio electrónico ya se daban antes de Internet , de manera que la mayor parte de los fraudes son tan antiguos como la vida misma; la novedad es la vía que se utiliza que, a diferencia de los fraudes anteriores, no tiene fronteras y, por tanto, son más difíciles de perseguir.

Las autoridades norteamericanas han alertado sobre los diez fraudes más habituales en el comercio electrónico, recomendando consejos generales que van desde la lectura atenta de los contratos, mostrarse escéptico ante empresas que no suministren su dirección postal y teléfono y desconfiar de las oportunidades[7].

Artículo 278.-

1. El que para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos y otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

[7] La Comisión Federal de Comercio de Estados Unidos ha publicado la lista de las 10 estafas más frecuentes que se cometen en el comercio electrónico.
1. Subastas. No subastarás aquel objeto que no tengas, y el que tengas lo has de enviar y si no, devolver el dinero inmediatamente. Las autoridades han perseguido a la empresa Computers By Us de Pensilvania por olvidar estos *detalles.*
2. Letra pequeña. Empresas que dan acceso a Internet ofrecen horas gratis a cambio de suscribirse por un año. La empresa asegura en su formulario de contrato que todo aquel que quiera podrá darse de baja en cualquier momento, pero en letra pequeña añaden interminables cláusulas entre las que cuales figura el precio que hay que pagar en caso de darse de baja. La FTC aconseja leer la letra pequeña.
3. Tarjeta de crédito. Hay empresas que solicitan el número de la tarjeta de crédito para cualquier trámite, como para hacer una reserva o comprobar que se trata de un usuario adulto (en sitios eróticos), pero ya empiezan a cargar comisiones sin aviso y sin haber prestado el servicio.

Un estudio de Cybersource y Mindwave afirma que mientras las compras con tarjetas de crédito han aumentado el 5% en los Estados Unidos, el fraude cometido con tarjetas ha crecido el 50%.

Una de las primeras inquietudes que asaltan a cualquier neófito en esta materia es la aparente vulnerabilidad de los sistemas y procedimientos de seguridad empleados en Internet .

¿Estamos ante un gigante con los pies de barro?. Muchas de las noticias vertidas recientemente en los medios de comunicación resultan ciertamente alarmantes. Por ejemplo, los ataques de la "hackers" durante el año 2.000 han causado daños a las empresas norteamericanas por valor de 266 millones de dólares (49.742 millones de pesetas), lo que supone el doble del año 1.999, según un estudio del Instituto de Seguridad Informática del FBI. Además, el número de ataques crece, buena prueba de ello es que en la primera mitad del año 2.000 se contabilizaron un total de 8.836 incidentes de seguridad, casi tantos como los registrados en todo 1.999 [8].

¿Quién no recuerda alguna noticia sobre "hackers" entrando hasta los archivos y lugares más recónditos de la NASA, el Pentágono o la propia Microsoft?

El diario *Wall Street Journal* daba la primicia de que unos desconocidos, gracias a un virus troyano, habían entrado en el sistema informático de la compañía Microsoft en Redmond. Se calculaba que, hasta haberse detectado la intrusión, podían haber estado husmeando durante tres meses y llegado al código fuente de algunos productos claves de la firma.

---

4. Cambio de dial. Un truco que va a más: ofrecer gratuitamente material para adultos, pero el sitio cambia la conexión del módem de acceso del usuario a un número de teléfono de larga distancia. La FTC recomienda vigilar la factura telefónica.
5. Albergue de páginas. Se ofrece el albergue en la red de una página personal gratuitamente durante 30 días de prueba. Se cobra el servicio aunque el cliente se haya dado de baja tras el período de prueba.
6. Pirámide. En Estados Unidos hay variantes del sistema de mercadotecnia piramidal prohibidas.
7. Vacaciones gratis. El gancho oculta comisiones, extras milagrosos que se multiplican por todas partes, y unas condiciones de hoteles en donde lo más inimaginable es la foto que te enviaron por la *web* .
8. Ofertas de empleo . Promesas de ganar dinero a cambio de comprar un material con la excusa de la formación profesional. Este dinero nunca será recuperado. Incluso es muy difícil tener la oportunidad de hablar con alguien de esa fantasiosa empresa.
9. Inversiones. Al calor de los *daytraders*, de los inversores aficionados y de los millonarios veinteañeros, algunas empresas ofrecen grandes ganancias en la Bolsa que nunca se producen. Y, aunque se produzcan, nunca llegan a tu bolsillo.
10. Curas milagrosas. En otros tiempos ofrecían por correo cremas para agrandar el busto o el pene, ahora por *e-mail* mandan pruebas para saber si tienes el SIDA y pócimas milagrosas. El consumidor nunca analizará la pócima que le envían. " (EL CIBERPAIS 9-11-2000)

[8] Diario EL PAIS, 3 de octubre de 2.000

La aparición de un virus informático en cualquier ordenador, sea particular sea de una empresa, es un hecho tan usual como traumático, que siempre acarrea pérdidas.

Dos factores han influido en el auge de la aparición y expansión de los virus informáticos: la creación de la World Wide Web, y el ataque constante que sufre el sector empresarial e incluso algunas instituciones.

El problema de los virus informáticos transmitidos por Internet tiene una doble dimensión desde el punto de vista de la responsabilidad civil en función del origen del contagio.

Pensemos en primer lugar en el supuesto del contaminador de virus que los crea y transmite con ánimo malintencionado. Este es un caso bastante claro en el que concurren los requisitos de la responsabilidad civil y posiblemente, según los antecedentes, también de la responsabilidad penal. Sin embargo resulta bastante más complejo de valorar el supuesto de transmisión de virus de forma involuntaria o concurriendo fuerza mayor (hecho imprevisible, inevitable ajeno al presunto responsable y de tal fuerza que suponga un obstáculo invencible para quien transmita un virus informático, por ejemplo, por medio del correo electrónico). En esta segunda hipótesis estaríamos hablando de un usuario de correo electrónico que transmite, sin saberlo, un virus previamente contraído por dicho correo, cuya detección resulta a todas luces imposible en el momento en el que se recibe y transmite a terceros por ser un virus aún no catalogado o por otra causa que impida su identificación con arreglo a la técnica normal requerida para el ejercicio de la actividad desarrollada. Posiblemente en este segundo supuesto no concurran los elementos de la responsabilidad, siempre y cuando el contagiado que transmita el virus no tenga la posibilidad material de haberlo detectado y evitar así el contagio posterior a otros terceros.

Uno de los estudios más relevantes realizado acerca de la problemática de los virus, es el realizado por la compañía norteamericana ICSA, encargada de cuantificar anualmente los daños producidos por los virus informáticos, sirva a modo de ejemplo de 300 compañías seleccionadas, el 99,67% han sufrido ataques de virus y que frente a 10 infecciones al mes por cada 1000 ordenadores en 1996, se ha pasado a 90 infecciones en el año 2.000.

El problema es de un calado extraordinario y puede comprometer seriamente la viabilidad de empresas, profesionales y Administraciones

Públicas, sobre todo si tenemos en cuenta el mal endémico de las pequeñas y medianas empresas en España a la hora de dedicar escasos recurso a la prevención de riesgos. Surge, como ya se ha apuntado, por la aparición de Internet , y la cantidad de posibilidades que la red ofrece, ya que si con anterioridad a la misma los virus que se creaban se expandían a través de ficheros, es decir, mediante el intercambio de software, posteriormente ese software se encontraba en la red y el intercambio se hizo innecesario.

Virus como *I love you* o *Melissa* traen en jaque a muchas empresas. El problema quizá reside en la importante inversión que debe realizar un empresario si quiere estar parcialmente a salvo de los virus, ya que no sólo debe proteger sus ordenadores con antivirus y con sus actualizaciones, sino también debe proporcionar a sus empleados la necesaria información (si es que no la tienen), acerca de las modalidades de agentes infecciosos y cómo enfrentarse a ellos, porque está comprobado que los mayores daños que causa uno de estos pequeños pero peligrosísimos virus son consecuencia de una errónea actuación de los afectados.

Por ello es imprescindible invertir en formación, conclusión a la que llegan muchas empresas, lamentablemente, sólo después de ser infectadas y sufrir pérdidas cuantiosas.

Igualmente surge la pregunta de la posible solución a la creación de virus cada vez más sofisticados y cuyas consecuencias pueden ser fatales, sirva como ejemplo la paralización de todo el sistema de Microsoft por el virus *I love you*. Esa respuesta es muy diversa según los Estados, y va desde una legislación penal enormemente dura, como es la norteamericana, al polo opuesto, como ocurrió en Taiwan con el creador del antedicho virus que no fue denunciado y consiguió un contrato con una conocida empresa fabricadora de antivirus.

No obstante, siempre queda la vía de la responsabilidad civil a la hora de reclamara los daños producidos por estos agentes, claro está, siempre y cuando sea identificable el agente causante del daño y concurran los requisitos de exigencia de responsabilidad.

II

La privacidad en Internet [9]

El artículo 18.4 de la Constitución Española instaura el imperativo legal de la *limitación del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.*

---

[9] La consideración que la intimidad tiene en los ordenamientos jurídicos occidentales, que la han venido considerando un bien jurídico susceptible de protección constitucional, nos permite hacernos una idea de la importancia de las intromisiones propiciadas por las nuevas tecnologías. La importancia de esta cuestión en sectores claves de la economía como el asegurador ya se destacó en el CEGERS de 1998, cuyo tema fue precisamente Riesgos informáticos y panorámica actual de otros grandes riesgos Cf. Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XV, nº 62, segundo trimestre de 1998

Otras publicaciones de interés son:

- Agencia de protección de datos: El Consejo de Europa y la protección de datos personales, Madrid, 1997.
- Lucas Murillo de la cueva, P: Informática y protección de datos personales. Estudio sobre la L.O. 5/1992, de Regulación de Tratamiento Automatizado de los Datos de Carácter Personal, Centro de Estudios Constitucionales, Madrid, 1993.
- Gay, C.: Intimidad y tratamiento de datos en las administraciones públicas, Editorial Complutense, Madrid, 1995.
- Agencia de protección de datos: Jornadas sobre el Derecho español de la protección de datos personales, Madrid, 28, 29 y 30 de Octubre de 1.996, , Madrid, 1997
- Ortí Vallejo, A.: Legislación de datos de carácter personal,. Tecnos, Madrid
- Delitos informáticos, número monográfico de la Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XIII, nº 51, tercer trimestre de 1995.
- Domaica Montoro, J.M.: El fraude informático, ¿un riesgo asegurable?, Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XII, nº 47, tercer trimestre de 1994
- Domaica Montoro, J.M., Riesgos de los delitos relacionados con las tecnologías de la información y las comunicaciones, Revista de Gerencia de Riesgos de la Fundación Mapfre Estudios, Año XV, nº 60, cuarto trimestre de 1997
- Garriga Domínguez, A.: La protección de los datos personales en el derecho español, , Dykinson, Madrid, 1999.
- Estadella Yuste, O.: La protección de la intimidad frente a la transmisión internacional de datos personales, , Tecnos, Madrid, 1995.

Este principio se encuentra recogido en el Proyecto de CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA establece que toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Estos datos se tratarán de modo leal, para fines determinados y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. El respeto de estas normas quedará sujeto al control de una autoridad independiente (Artículo 8. De la Ley Protección de datos de carácter personal) [10]

El derecho a la intimidad garantizado en el art. 18.1 CE, que se identifica con el derecho de toda persona a no ser objeto de injerencias arbitrarias en su vida privada y familiar, reconocido con términos casi idénticos en los arts. 12 Declaración Universal de Derechos Humanos de 10 Dic. 1948, 8.1 Convenio de Roma 4 Nov. 1950 (protección de los derechos humanos y de las libertades fundamentales) y 17.1 Pacto Internacional de Derechos Civiles y Políticos de 19 Dic. 1966, se concreta, por lo que al ordenamiento español se refiere, en el art. 18.2, 3 y 4 CE, en el que se encuentra el reconocimiento de la inviolabilidad del domicilio, la garantía del secreto de las comunicaciones y la previsión de una ley que limite el uso de la informática en defensa de, entre otros derechos, la intimidad personal de los ciudadanos.[11]

Se trata de evitar que la informatización de los datos personales propicie comportamientos discriminatorios. El art. 18.4 CE no sólo entraña

---

[10] La Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (L.O.R.T.A.D.), de 29 de Octubre de 1.992, derogada por la **Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal**, vino a dar cumplimiento con cierto retraso al precepto contenido en el artículo 18.4 de la Constitución Española, de 6 de Diciembre de 1.978, según el cual:

> **"La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."**

El ámbito de aplicación de la Ley 15/1999 se refiere a los datos de carácter personal 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. En consecuencia, **se rigen por esta Ley Orgánica todo tratamiento de datos de carácter personal:**

> a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
> b) Cuando el responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho internacional público.
> c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito (art. 2)

[11] TS. TRIBUNAL SUPREMO (Sala 2) 05/11/1999 Granados Pérez

un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona --a la "privacidad"--, pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos.

De tal manera que está prohibido tajantemente el uso de los datos para finalidades distintas de las que motivaron su recogida, así como su exactitud y puesta al día, siendo este un principio general de la protección de datos, la congruencia y racionalidad de su utilización, en cuya virtud ha de mediar una nítida conexión entre la información personal que se recaba y trata informáticamente y el legítimo objetivo para el que se solicita y, en consecuencia.

El art. 18.1 de la Constitución Española garantiza "el derecho al honor, a la intimidad personal y familiar y a la propia imagen" reuniendo así tres derechos diferentes en razón de que en muchas ocasiones hay un nexo o conexión entre ellos, y por ello la LO 1/1982 de 5 May. (protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen) unifica su protección civil. No obstante, dichos derechos continúan siendo diferentes, de manera que no estamos de un derecho tricéfalo, sino ante tres derechos diferenciados, como diferentes pueden ser los ataques a los mismos, ya que el derecho al honor se refiere a la estimación de la persona en y por la sociedad y contribuye a configurar el estado social de la misma; el derecho a la intimidad personal y familiar se refiere a una vida secreta y privada de la persona sustraída a indagaciones ajenas; y el derecho a la propia imagen se refiere en su esencia a poder impedir la reproducción de la figura humana en cualquier medio de expresión.

En la sociedad actual, con el desarrollo acelerado de la informática, las comunicaciones y las redes abiertas, la limitación y protección que impone el meritado artículo de nuestro texto constitucional, puede chocar con el creciente tratamiento automatizado de los datos de carácter personal, tratamiento que tiene también encuadre constitucional, concretamente en el artículo 20 (libertad de expresión e información). Conforme a la declaración programática del art. 18.1 CE, los derechos al honor, a la intimidad personal y familiar y a la propia imagen, de incuestionable rango constitucional, ofrecen suficiente entidad para que, a tenor del art. 20.4 CE, vengan a constituir un verdadero límite al ejercicio de la libertad de expresión, y de ahí que la LO 1/1982 de 5 May. (protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen), al fijar el ámbito en que han de desenvolverse los derechos regulados en el

art. 2, enumera una serie de supuestos de vulneración de tales derechos y en su art. 7.7 recoge como supuesto de intromisión ilegítima la divulgación de expresiones o hechos concernientes a una persona cuando implique difamación o desmerecimiento en la consideración ajena.

Los derechos al honor, a la intimidad personal y familiar y a la propia imagen son derechos subjetivos que no tienen, a diferencia de los restantes derechos fundamentales, el carácter de irrenunciables en cuanto que la autorización o el consentimiento de las violaciones de los mismos hecha por el ofendido supone una renuncia a la tutela legal (art. 1 LO 1/1982 de 5 May., protección del derecho al honor, a la intimidad personal y familiar y a la propia imagen), pero si esto no ocurre, la intromisión ilegal producida da lugar a la correspondiente indemnización, ya que la LO 1/1982 citada establece, en su art. 9, una objetivización del daño derivado de la intromisión ilegal al presumirlo en todo caso.

Surge así el problema de la protección del ámbito personal de los ciudadanos, frente a los "ataques" que provienen de los medios telemáticos e informáticos. Y no se trata sólo de proteger datos, sino de proteger lo que en términos anglosajones se conoce como privacy (privacidad en castellano), concepto que engloba tanto el conjunto de datos de una persona, como el perfil que de ella se puede obtener a partir de los mismos.

El derecho al honor, protegido como derecho fundamental en nuestra Constitución, carece de definición legal. En la doctrina, se ha aceptado unánimemente la definición italiana que lo conceptúa como una dignidad personal reflejada en la consideración de las demás y en el sentimiento de la propia persona. La doctrina del alto Tribunal sobre el derecho al honor añade la nota de que dicho derecho debe estar afectado por una tarea de ponderación con relación a la **libertad de información**, teniendo en cuenta la posición prevalente, que no jerárquica o absoluta, de ésta. Así se debe proclamar, puesto que la libertad de información del art. 20.1.d) CE además de tener el carácter de una libertad individual, indica que una opinión pública libre está indisolublemente unida al pluralismo político dentro de un Estado democrático y al principio de legitimidad democrática que proclama el art. 1.2 CE y que es la base de toda la ordenación jurídico-política.

Es perfectamente posible hoy en día, obtener determinada información uniendo e hilando todos y cada uno de los pequeños datos que cada uno vamos dejando tanto en medios informáticos como de comunicación, información que se obtiene con las posibilidades que ofrecen los modernos medios tecnológicos y que ya no es la original, sino

una nueva, surgiendo entonces la pregunta de la titularidad, y por consiguiente, el poder sobre esa nueva información.

Ciertamente la opinión tiene más fuerza que la verdad y como dice la Exposición de Motivos de la Ley Orgánica 2/1997 de 16 de junio: *"La información no puede ser objeto de consideraciones mercantilistas, ni el profesional de la información puede ser concebido como una especie de mercenario abierto a todo tipo de informaciones y noticias que son difundidas al margen del mandato constitucional de veracidad y pluralismo"*. De ahí que dicha Ley responde a la necesidad de otorgar a los profesionales de la información un derecho básico en la medida en que ellos son el factor fundamental en la producción de informaciones. Su trabajo está presidido por un indudable componente intelectual, que ni los poderes públicos ni las empresas de comunicación pueden olvidar.

El derecho fundamental a la intimidad, que aparece consagrado en el art. 18.1 CE, impide las injerencias en la intimidad «arbitrarias o ilegales», y sólo la ley puede autorizar intromisiones por «imperativos de interés público». Todo derecho tiene sus límites, establecidos, en relación a los derechos fundamentales, en algunas ocasiones, por la propia CE, mientras que en otras ocasiones el límite deriva de una manera mediata o indirecta de tal norma, en cuanto ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionales protegidos

Ante estas realidades, es necesaria una protección eficaz, protección que tiene dos vertientes: defensa de los derechos que posee sobre la información su titular, y conocimiento de los ciudadanos, tanto de esos derechos, como de los niveles de confidencialidad que puede exigir en el tratamiento de sus datos.

La primera vertiente de la protección señalada, tiene reflejo en la legislación española e igualmente en el Derecho comparado. Esta vertiente no presenta excesivos problemas, pues prácticamente todas las legislaciones occidentales reconocen el derecho a decidir cuándo y cómo se va a utilizar la información que en unos casos se proporciona de manera voluntaria y otras por imperativo legal. Buen ejemplo de ello lo encontramos en nuestra Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, ley que se caracteriza por su carácter moderno e innovador.

Pero es la otra vertiente de la protección la que presenta los mayores problemas, y sin la cual la defensa de los derechos que amparan la

privacidad no resulta todo lo eficiente que debería ser: es precisamente el conocimiento del tratamiento de sus datos que puede llegar a exigir, lo que da virtualidad a la existencia de una defensa de los derechos que posee sobre ellos, podríamos decir que la información sobre el tratamiento de la información es lo que permitirá una respuesta eficaz y un cumplimiento escrupuloso de la obligación constitucional que recoge el artículo 18.

La Fiscalía General del Estado ha manifestado preocupación respecto de las distintas repercusiones penales por el tratamiento telemático y sus repercusiones en en relación con los derechos de artículo 18 de la Constitución.

Fruto de esta preocupación es la Circular 1/1.999 de la mencionada Fiscalía en la que: "La Fiscalía consultante somete a consideración un delicado problema interpretativo que además de cuestionar el alcance recíproco de dos derechos fundamentales íntimamente relacionados como son la libertad e inviolabilidad de las comunicaciones —art. 18.3 de la Constitución Española— y la libertad informática —art. 18.4 de la Constitución Española—, afecta también de modo directo a la definición de los límites que el Derecho positivo asigna a las facultades de investigación autónoma que el Ministerio Fiscal tiene atribuidas en el art. 5 del Estatuto Orgánico del Ministerio Fiscal."

Encabeza la consulta una interesante disquisición sobre las necesidades prioritarias que plantea la represión de una categoría nueva de delitos como son los relacionados con el uso de la informática.

El hecho particular que suscita la consulta se refiere a una empresa de sistemas informáticos que sufre un acceso indebido a sus ordenadores por parte de personas no identificadas que provocan el borrado de diversos ficheros.

La investigación e instrucción de la causa requiere en estos casos como primera diligencia la identificación de los abonados desde cuyos teléfonos o terminales se han realizado las conexiones telemáticas, lo que obliga a acudir al operador del servicio telefónico para recabar la información correspondiente.

En el caso que nos ocupa el Fiscal de propia autoridad y en el marco de una investigación preprocesal solicita del operador telefónico el conocimiento

de los números de abonado desde los que se verificaron las conexiones presuntamente criminosas.

La compañía operadora entiende que la información solicitada afecta al estatuto constitucional de inviolabilidad de las comunicaciones —art. 18.3 de la Constitución Española— y deniega el acceso a los datos en tanto no medie resolución judicial.

La consecuencia colateral de esta postura obstativa implica una restricción de las facultades de investigación del Fiscal en la medida en que el art. 5.2 del Estatuto Orgánico reduce la legitimación para la adopción de medidas de investigación a aquellas que no sean limitativas de derechos, por lo que la selección del régimen constitucional de garantía que le cuadra a este tipo de datos y contenidos, sea el estatuto de inviolabilidad del art. 18.3 de la Constitución Española, sea la libertad informática del art. 18.4 de la Constitución Española, repercute de inmediato en la afirmación de la existencia o inexistencia de posibilidades de investigación autónoma por parte del Ministerio Fiscal.

La Fiscalía de procedencia se pronuncia sobre la cuestión y estima que el estatuto de inviolabilidad sólo opera cuando el acto de comunicación es interceptado en tiempo real, esto es, mientras se produce la transferencia del mensaje, pues considera que el bien protegido es el libre flujo de las comunicaciones, de modo que, extinguida la comunicación, los datos que se registran en soporte informático para la facturación del servicio prestado quedarían sujetos al régimen específico del art. 18.4 de la Constitución Española y de la Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, que no exige habilitación judicial para la cesión de información en favor del Ministerio Fiscal —art. 11.2 d)—.
También estima que la legislación de telecomunicaciones distingue conceptualmente entre interceptación de contenidos y acceso a los datos de tráfico, entre los que se incluyen los datos de identidad de los comunicantes, y que de conformidad con el art. 51 de la Ley 11/1998 de 24 de abril, General de Telecomunicaciones, sólo la interceptación del contenido exige licencia judicial, lo que a sensu contrario conduce a estimar no abarcados en el secreto de las comunicaciones los aspectos e informaciones no comprendidos en el contenido mismo. Se cita asimismo el art. 3.2 de la Ley 24/1998 de 19 de julio, del Servicio Postal Universal, que en relación con los datos sobre la existencia del envío, clase, identidad del remitente y destinatario, y sus direcciones, remite a la aplicación de la Ley Orgánica 5/1992 de 29 de octubre.

Concluye finalmente la Circular de la Fiscalía que: "El Ministerio Fiscal no puede inmiscuirse en datos incorporados al contenido sustancial del derecho fundamental al secreto de las comunicaciones sin licencia judicial. Exigir del operador telefónico la identificación de los números de abonado conectados en una concreta y determinada comunicación supone una restricción de derechos prohibida por el art. 5.2 del Estatuto Orgánico del Ministerio Fiscal, por lo que es preciso acudir al Juez de instrucción, justificar la necesidad de la medida e instar la incoación de diligencias previas. Si el proceso está en curso, el Fiscal también debe solicitar del Juez de instrucción la adopción de la resolución judicial legitimadora de la injerencia. Ni las diligencias de investigación preprocesal amparadas en los arts. 5 del Estatuto Orgánico del Ministerio Fiscal y 785 bis de la Ley de Enjuiciamiento Criminal, ni las posibilidades de investigación autónoma paraprocesal que cabe deducir de los arts. 781.2 y 792.1.2 de la Ley de Enjuiciamiento Criminal constituyen marco legal idóneo para exigir del operador de la red o del prestador del servicio la revelación de los datos de tráfico registrados en las comunicaciones establecidas."

Aún queda mucho camino por recorrer, pues es escasa, por no decir inexistente, la información que sobre la manipulación de los datos que vamos dejando en los medios telemáticos e informáticos se nos proporciona en nuestros tiempos, así como de las consecuencias que puede tener tanto suministrar esos datos, como de las acciones que se pueden llevar a cabo en el probable caso de que nos encontremos con un tratamiento que atente contra nuestra privacidad. Quién no ha recibido alguna vez publicidad, tanto por medio del correo ordinario, como por el moderno correo electrónico, de empresas u otras entidades y se ha preguntado cómo y de dónde han sacado nuestra dirección.[12]

Pues bien, si la educación sobre el tema de la protección de la privacidad es escasa y en ocasiones controvertida en los círculos jurídicos, donde sólo los interesados realmente en esta cuestión buscan información sobre ella y se preparan en profundidad, la educación para el resto de los ciudadanos es

[12] En previsión de los nuevos riesgos que el tratamiento automatizado de datos personales pueda originar para la plena efectividad de los derechos de los ciudadanos, se dispone en el art. 18.4 CE que «la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Se trata, por tanto, de un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos. De suerte que un sistema normativo que, autorizando la recogida de datos incluso con fines legítimos, y de contenido aparentemente neutro, no incluyese garantías adecuadas frente a su uso potencialmente invasor de la vida privada del ciudadano, a través de su tratamiento técnico, vulneraría el derecho a la intimidad de la misma manera en que lo harían las intromisiones directas en el contenido nuclear de ésta. TC. TRIBUNAL CONSTITUCIONAL (Sala 1) 08/11/1999 Cachón Villar

totalmente nula, y es en este campo desde el que debería empezarse a actuar si realmente se quiere llegar a una máxima protección del derecho a la intimidad, así como a la elección por parte de cada uno del grado de confidencialidad con el que sean tratados los inevitables rastros que sobre sí mismo va dejando en el mundo de las telecomunicaciones.

Secreto de las comunicaciones. Acceso no consentido al correo electrónico.-

El artículo 18.3 de la Constitución Española establece que: "*Se garantiza el derecho de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial*".

Esta norma contiene el derecho fundamental del individuo frente al Estado, afirmando el derecho al secreto, plasmación singular de los principios declarados en el art. 10.1 CE --dignidad de la persona y afirmación del libre desarrollo de su personalidad como fundamento del orden público y de la paz social--, y que se encuentra íntimamente vinculado al derecho a la intimidad, pero sin confundirse plenamente, ya que toda comunicación es para la norma fundamental secreta y sólo algunas, como es obvio, serán íntimas y privadas.

En esta misma línea el Proyecto de CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA establece que toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y del secreto de sus comunicaciones (Artículo 7. Respeto a la vida privada y familiar)

La polémica está servida respecto del problema de los correos electrónicos de empleados, dependientes y funcionarios de empresas y Administraciones Públicas.

En este orden de cosas convendría distinguir dos supuestos bien diferenciados: El uso de la cuenta de correo electrónico que presta la empresa y la conexión desde la empresa a una cuenta personal de correo que el trabajador tenga abierta en la red. Mientras en el primer caso existen opiniones divididas sobre si se puede inspeccionar o no el contenido del correo electrónico, en el segundo no, ya que nos encontramos ante un acto privado autorizado por el empresario por lo que el mismo deberá respetar su privacidad.

Recientemente los medios de comunicación se han hecho eco del proyecto británico de autorizar a los empresarios la inspección rutinaria del correo electrónico que sus trabajadores envían desde el lugar de trabajo sin otro requisito que la previa advertencia a los mismos.

En el debate hay tres posiciones claramente diferenciadas, en primer lugar la de quienes defienden el derecho del empleador a rastrear el correo de sus trabajadores, en segundo lugar la de quienes limitan el derecho de inspección del empleador a la existencia de sospecha y a una apertura con garantías para el empleado y finalmente aquellos que defienden la tesis de la imposibilidad de inspección sistemática e indiscriminada de los correos electrónicos de los dependientes por atentar tanto al artículo 18.3 de la Constitución Española como al artículo 197 del Código penal.

A la hora de valorar estas posibles alternativas conviene no olvidar que la intimidad personal puede llegar a ceder en ciertos casos y en cualquiera de sus diversas expresiones ante exigencias públicas, pues no es un derecho de carácter absoluto, pese a que la CE, al enunciarlo, no haya establecido de modo expreso la reserva de intervención judicial que figura en las normas declarativas de la inviolabilidad del domicilio o del secreto de las comunicaciones (art. 18 núms. 2 y 3 CE); tal afectación del ámbito de la intimidad es posible sólo por decisión judicial, que habrá de prever que su ejecución sea respetuosa de la dignidad de la persona y no constitutiva, atendidas las circunstancias del caso, de trato degradante alguno (arts. 10.1 y 15 CE).[13]

El principio de respeto a la intimidad personal y a las comunicaciones privadas, frente a injerencias de las autoridades públicas, puede ceder, excepcionalmente, con el fin de proteger otros valores sociales que hayan de sobreponerse a los derechos individuales. Así el art. 8 Convenio de Roma 4 Nov. 1950 (protección de los derechos humanos y de las libertades fundamentales) señala la posibilidad de excepción cuando la injerencia esté prevista legalmente y se plasme en medidas necesarias en una sociedad democrática para la protección de intereses generales o colectivos como son, entre otros, la seguridad pública, la defensa del orden y la protección de los derechos y libertades de los demás ciudadanos. Consecuentemente con ese principio, el art. 18.3 CE prevé la salvedad de que por resolución judicial proceda adoptar excepciones a la garantía del secreto de las comunicaciones postales, telegráficas y telefónicas. En relación con esa posibilidad, la LO 4/1988 de 25 May. (reforma de la LECrim. en materia de delitos relacionados con bandas armadas o elementos terroristas o

[13] TC. TRIBUNAL CONSTITUCIONAL (Sala 1) 15/02/1989 Rubio Llorente

rebeldes) introdujo la redacción del art. 579 núms. 2 y 3 LECrim., conforme al cual es posible la intervención de las comunicaciones telefónicas de los procesados o personas de las que hubiere indicios de responsabilidad criminal, siempre que por esa intervención se pudiera obtener el descubrimiento o comprobación de hechos o circunstancias importantes de la causa y con la exigencia de que la intervención se acuerde por resolución motivada. Si se tienen en cuenta tales precauciones, con las aclaraciones que la jurisprudencia ha señalado, no se producirá violación de derechos o libertades fundamentales que invalidaría la eficacia de las pruebas, directa o indirectamente derivadas de tal violación [14].

En otro medio de comunicación como son las comunicaciones telefónicas, ya existe una línea jurisprudencial que permite esclarecer cuando se puede o no intervenir una línea telefónica, Así, son requisitos de las intervenciones telefónicas tanto para evitar la infracción del derecho al secreto de las comunicaciones constitucionalmente garantizado, como las que han de reunirse para que puedan ser acogidas como prueba: a) que esté prevista legalmente y que constituya una necesidad para la protección de intereses colectivos o generales como son la seguridad nacional y pública, la defensa del orden y la protección de derechos y libertades de los ciudadanos; b) de conformidad con la exigencia que expresa el art. 18.3 CE, ha de ser acordada en todo caso judicialmente y con una finalidad exclusiva de descubrir la existencia de delito y quienes sean las personas responsables del mismo; c) deben acotarse con precisión los teléfonos sobre los que recaiga la intervención, que habrán de ser los de las personas que puedan aparecer indiciariamente implicadas o de los que se sirvan habitualmente; d) la medida ha de ser excepcional en el sentido de que habrá de recurrirse a ella cuando no haya otro medio de investigación menos lesivo de los derechos individuales, proporcionada a la gravedad de los hechos cuya averiguación se pretende, temporalmente limitada sin que pueda admitirse intervenciones indefinidas o de duración excesiva, siendo inadmisible las que se encaminen a una averiguación indiscriminada de delitos, acordada en un procedimiento de investigación criminal o determinadora de su inicio, basarse imprescindiblemente en verdaderos indicios que permitan, aun cuando no sean datos exhaustivos, afirmar se cuenta con noticia racional de la existencia de delito, no bastando meras sospechas o conjeturas, y acordarse por resolución motivada que se refiera a las circunstancias concretas del caso en que la supresión de la protección constitucional se acuerde [15].

---

[14] TS. TRIBUNAL SUPREMO (Sala 2) 22/01/1996 Martín Canivell

[15] TS 2.ª SS 8 y 26 May., 26 Jun. 1997 y 20 Jun. 1998.

Como expone la sentencia del Tribunal Constitucional 114/1984 de 29 de noviembre, en su fundamento jurídico séptimo, el derecho fundamental a la libertad y secreto de las comunicaciones puede conculcarse tanto por la interceptación en sentido estricto —que suponga aprehensión física del soporte del mensaje, con conocimiento o no del mismo, o captación del proceso de comunicación— como por el simple conocimiento antijurídico de lo comunicado —apertura de la correspondencia ajena guardada por el destinatario, por ejemplo—, porque la Constitución protege no sólo el proceso de comunicación, sino también el mensaje, en el caso de que éste se materialice en algún objeto físico, y el objeto del secreto abarca no sólo el contenido de la comunicación, sino también otros aspectos de la misma, como por ejemplo la identidad subjetiva de los interlocutores o corresponsales.

Lo que indica la doctrina constitucional y del Tribunal de Estrasburgo es que no se pueden disociar sin merma relevante de garantías realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión.

El artículo 197 del Código Penal, que castiga a quien vulnere las comunicaciones personales. Este artículo cita el correo electrónico, una herramienta que no pudo prever la Constitución Española por su antigüedad, ni el Estatuto de los Trabajadores cuando reguló el registro de los efectos personales de los trabajadores.

El art. 18.3 de la Constitución Española consagró explícitamente el secreto de las comunicaciones, e implícitamente la libertad de las mismas, de lo que se deduce que la inmunidad constitucional no sólo previene la interceptación o captación en tiempo real, sino cualquier forma de conocimiento antijurídico del contenido del mensaje o de las circunstancias significativas de la comunicación, aunque se produzca fuera del contexto temporal de la conexión.

Por todo ello en nuestra opinión creemos que la protección constitucional de la intimidad cubre este vacío, de manera que:

1°.- Cuando el empleado verifique la conexión desde la empresa a una cuenta personal de correo que el trabajador tenga abierta en la red, el empresario no podrá tener acceso a la misma

2°.- Cuando es la empresa quien presta el correo como herramienta de trabajo, "y a esos únicos fines", se presenta un supuesto distinto, pero,

dado que no hay nada regulado, "ni en este caso" estaría justificado vulnerar la intimidad.

Sin perjuicio de ello y dado que el empresario no puede inmiscuirse en el correo electrónico ni en datos incorporados al contenido sustancial del derecho fundamental al secreto de las comunicaciones sin la preceptiva licencia judicial, podrá instar la correspondiente autorización judicial tomando, si lo estima oportuno, las medidas cautelares que, ajustándose a la legalidad, eviten la destrucción de las pruebas que acrediten la posible utilización indebida del correo o la conducta delictiva o desleal del empleado.

III

El comercio electrónico.-[16]

El comercio electrónico se basa en gran medida en los llamados contratos electrónicos.

En este tipo de contratos las condiciones no siempre están mutuamente negociadas. De hecho en un porcentaje muy alto nos encontramos ante condiciones generales de contratación unilateralmente redactadas por una de las partes que propone a la otra parte, la adhesión sin más a dichas condiciones.

Por ejemplo, un sistema de contratación muy empleado en Internet se basa en contratos llamados click-wrap —textos que aparecen forzosamente

---

[16] La irrupción de las muevas tecnologías de la información y, en general, el fenómeno globalizador, han configurado lo que se ha dado en llamar la *nueva economía*. En ella, la contratación electrónica juega, sin duda, un papel esencial. A este respecto, pueden señalarse algunas `publicaciones de interés:

- Oliver Cuello, R.: El comercio electrónico: perspectiva tributaria Actualidad informática Aranzadi, nº 33, octubre de 1999
- Sardina Ventosa, F.:La contratación electrónica del seguro de vida, Dykinson. Madrid, 2000.
- Carrascosa López, V., Del pozo Arranz, M.A.; y Rodríguez de Castro, E.P.: La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos, Comares. Granada, 1997.
- Martínez Nadal, A.: Comercio electrónico, firma digital y autoridades de certificación, Dykinson. Madrid, 1998.
- Martínez Nadal, A: Medios de pago en el comercio electrónico, Actualidad informática Aranzadi, nº 37, octubre de 2000
- Paz, E.: Cómo exportar, importar y hacer negocios a través de Internet Editorial Gestión 2000.Madrid, 2000.
- Barriuso Ruiz C.: La contratación electrónica. Aspecto legal del comercio electrónico, de loscontratos informáticos y del negocio jurídico por medios electrónicos, Dykinson. Madrid, 1998.
- Mougayar, W.:Nuevos mercados digitales. Comercio en Internet , Fundación Universidad – Empresa, Madrid. 1998.
- Oliver Cuello, R.: Tributación del Comercio Electrónico, . Tirant lo Blanch. Valencia, 1999.
- Álvarez-Cienfuegos Súarez, J.M.: Banca electrónica. LA LEY, 1997-3.

en la pantalla del ordenador en algún momento de la transacción—. Dichos documentos aparecen en la pantalla del ordenador indicando las condiciones y cláusulas del contrato, de manera que quien propone su condicionado requiere que el consumidor acepte dichas condiciones antes de proceder a la siguiente pantalla.

Nos encontramos sin duda ante una fuente inagotable de conflictos.

La Ley de condiciones generales de contratación -Ley 13-4-1998, núm. 7/1998- tiene por objeto -según indica el preámbulo de su exposición de motivos- la transposición de la Directiva 93/13/CEE, del Consejo, de 5 de abril de 1993, sobre cláusulas abusivas en los contratos celebrados con consumidores, así como la regulación de las condiciones generales de la contratación, y se dicta en virtud de los títulos competenciales que la Constitución Española atribuye en exclusiva al Estado en el artículo 149.1.6.ª y 8.ª, por afectar a la legislación mercantil y civil.

Se ha optado por llevar a cabo la incorporación de la Directiva citada mediante una Ley de Condiciones Generales de la Contratación, que al mismo tiempo, a través de su disposición adicional primera, modifique el marco jurídico preexistente de protección al consumidor, constituido por la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

La protección de la igualdad de los contratantes es presupuesto necesario de la justicia de los contenidos contractuales y constituye uno de los imperativos de la política jurídica en el ámbito de la actividad económica. Por ello la Ley pretende proteger los legítimos intereses de los consumidores y usuarios, pero también de cualquiera que contrate con una persona que utilice condiciones generales en su actividad contractual.

Se pretende así distinguir lo que son cláusulas abusivas de lo que son condiciones generales de la contratación.

Una cláusula es condición general cuando está predispuesta e incorporada a una pluralidad de contratos exclusivamente por una de las partes, y no tiene por qué ser abusiva. Cláusula abusiva es la que en contra de las exigencias de la buena fe causa en detrimento del consumidor un desequilibrio importante e injustificado de las obligaciones contractuales y puede tener o no el carácter de condición general, ya que también puede darse en contratos particulares cuando no existe negociación individual de sus cláusulas, esto es, en contratos de adhesión particulares.