7

5063/00/ES/FINAL
WP 37

Documento de trabajo

Privacidad en Internet:
- Enfoque comunitario integrado de la protección de datos en línea -

Adoptado el 21 de noviembre de 2000

Este Grupo de Trabajo, instituido por el artículo 19 de la Directiva 95/46/CE, es el organismo comunitario independiente de asesoramiento en materia de protección de datos y de la intimidad. Sus tareas están establecidas en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE. De las funciones de secretaría se encarga:

Unidad de libre circulación de la información y protección de datos, DG Mercado Interior, Comisión Europea
Rue de la Loi/Wetstraat 200, B-1049 Bruselas - Bélgica - Despacho: C100-2/133
Dirección de Internet: www.europa.eu.int/comm/dg15/en/media/dataprot/index/htm

Índice

CAPÍTULO 1: INTRODUCCIÓN

Este documento pretende ofrecer un enfoque comunitario integrado de la cuestión de la protección de datos en línea. La palabra "integrado" subraya que el análisis se basa principalmente en los textos de la Directiva general sobre protección de datos (Directiva 95/46/CE) y de la Directiva relativa a las telecomunicaciones y a la intimidad (Directiva 97/66/CE), aunque también se tienen en cuenta y se recogen todos los dictámenes y documentos que el Grupo de Trabajo ha adoptado hasta el momento sobre determinadas cuestiones importantes relacionadas con este tema[1].

Al debatir las prioridades del trabajo futuro, el Grupo de Trabajo ha defendido en varias ocasiones la necesidad de tratar las cuestiones sobre protección de datos relacionadas con el uso de Internet. En 1999, con el fin de abordar estos asuntos de una forma eficaz y sistemática, se creó el Grupo operativo sobre Internet, cuyo objetivo primordial es reunir los recursos y las experiencias técnicas de las distintas autoridades nacionales en materia de protección de datos y contribuir así a la interpretación y la aplicación uniformes de la normativa vigente en este campo.
El Grupo operativo sobre Internet ha redactado varios documentos que a lo largo de los dos últimos años ha adoptado el Grupo de Trabajo. Desde principios de 2000, el Grupo operativo sobre Internet se ha reunido con mayor frecuencia con vistas a alcanzar un documento de síntesis que pueda servir como referencia a la hora de tratar las cuestiones actuales, y en la medida de lo posible también las futuras, relacionadas con la intimidad en Internet.

El objetivo principal de este documento es ofrecer un primer enfoque de la cuestión de la privacidad en línea que pueda contribuir a aumentar la sensibilización respecto a los riesgos que el uso de Internet supone para la intimidad y que, al mismo tiempo, sirva de guía para interpretar las dos Directivas existentes en este campo. El Grupo de Trabajo es consciente de que la protección de la privacidad es una de las mayores preocupaciones de los usuarios de la Red[2]. Por lo tanto, concede una especial atención al tratamiento de este

[1] En particular: Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles abierta (OPS), adoptado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 16 de junio de 1998; Documento de trabajo: Tratamiento de datos personales en Internet, aprobado por el Grupo de Trabajo el 23 de febrero de 1999, WP 16, 5013/99/ES/final; Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, adoptado por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17; Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18; Dictamen n°3/99 relativo a información del sector público y protección de datos personales, aprobado por el Grupo de Trabajo el 3 de mayo de 1999; Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicios de Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999, 5085/99/ES/final, WP 25; Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, 5007/00/ES/final, WP 28; WP 29: Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, WP 29, 5009/00/ES/final; Dictamen 5/2000 sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multicriterio (guías inversas), WP 33, adoptado el 13 de julio de 2000, y Dictamen 7/2000 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas de 12 de julio de 2000, COM (2000) 385, adoptado el 2 de noviembre de 2000, WP 36.

[2] Así se ha señalado en un estudio semestral recientemente publicado por la Fundación Markle. Véase el artículo de AARON, D., *A Euro-American proposal for privacy on the Net,* Washington Post, 2 de agosto de 2000.

asunto, aunque reconoce que determinadas cuestiones polémicas, que suscitan un debate especial, pueden requerir un mayor trabajo en el futuro.

- Este documento no pretende ser exhaustivo en sí mismo, pero intenta cubrir las situaciones más habituales a las que pueden enfrentarse los usuarios de Internet cuando utilizan alguno de los servicios disponibles en la Red, tales como el correo electrónico, los navegadores, los buscadores, los foros de debate, etc. Debido a su carácter general, tampoco aborda cuestiones específicas que pueden requerir un estudio más detallado del Grupo de Trabajo en el futuro, como el control del correo electrónico en el puesto de trabajo. Este documento de trabajo se basa en el estado actual de Internet, que es, por naturaleza, un fenómeno enormemente dinámico y cambiante.

Para facilitar la lectura del documento, en primer lugar se abordan la descripción técnica básica y las cuestiones jurídicas generales. Posteriormente se trata por separado cada uno de los distintos servicios de Internet, analizando en cada capítulo las cuestiones técnicas y jurídicas pertinentes. Otro capítulo se dedica a las medidas y tecnologías en favor de la privacidad que pueden utilizarse para incrementar la privacidad de los usuarios de Internet. El último capítulo presenta las conclusiones.
Al final del documento se incluye un glosario de términos técnicos para facilitar a los lectores la comprensión de los conceptos técnicos utilizados en el texto. Las palabras contenidas en el glosario aparecen en el texto destacadas en cursiva.

El Grupo operativo sobre Internet ha decidido deliberadamente mantener cierto grado de superposición en el documento, lo que permitirá a los lectores con especial interés en un tema específico realizar una lectura selectiva. Para ello se han mantenido en el texto algunas descripciones adicionales, repetitivas en ocasiones, destinadas a simplificar la consulta de los distintos capítulos.

La coordinación del trabajo del Grupo operativo sobre Internet ha sido responsabilidad de Peter HUSTINX, presidente de la autoridad holandesa responsable de la protección de datos. Un grupo de redacción nombrado en el seno del Grupo operativo sobre Internet y formado por Diana ALONSO BLAS (de la autoridad holandesa de protección de datos) y Anne-Christine LACOSTE (de la autoridad belga de protección de datos) ha preparado la versión consolidada del documento de trabajo. Entre las tareas que ha realizado este grupo de redacción cabe destacar la estructuración y el control de la coherencia de todo el documento, la integración y el posterior desarrollo de las cuestiones jurídicas adicionales y de la información técnica y los comentarios recibidos de otras delegaciones, la elaboración del glosario de términos técnicos y la redacción de las conclusiones del documento.

Delegados de las autoridades responsables de la protección de datos de seis países han participado en diferentes fases del trabajo del Grupo operativo sobre Internet, redactando textos que han servido de base para varios capítulos, comentando las aportaciones de otros miembros del Grupo operativo sobre Internet e interviniendo en los debates que tuvieron lugar durante las cinco reuniones que el Grupo operativo celebró en 2000.
Cabe mencionar en especial a Anne-Christine Lacoste y Jean-Marc Dinant (Bélgica), Ib Alfred Larsen (Dinamarca), Marie Georges (Francia), Angelika Jennen y Sven Moers (Alemania), Emilio Aced Félez (España) y Diana Alonso Blas, Ronald Hes y Bernard Hulsman (Países Bajos). El Grupo operativo sobre Internet desearía expresar su agradecimiento a Christine Sottong-Micas (Secretaría del Grupo de Trabajo sobre

protección de datos del artículo 29 de la Comisión Europea) y Karola Wolprecht (prácticas 1999/2000 en la Comisión Europea) por su ayuda y su asistencia.

CAPÍTULO 2: DESCRIPCIÓN TÉCNICA DE INTERNET

I. Nociones básicas

Internet es una red de ordenadores que se comunican entre sí utilizando el *protocolo* de control de transporte/*protocolo* de Internet (TCP/IP)[3]. Se trata de una red internacional de ordenadores interconectados que permite a millones de personas comunicarse unas con otras en el "ciberespacio" y acceder a inmensas cantidades de información procedente de todo el mundo[4].
El predecesor histórico de Internet fue la red militar ARPAnet (1969). La idea básica era construir una red estadounidense digitalizada que permitiese a los ordenadores del ejército, de los contratistas que trabajaban para el ejército y de las universidades participantes en investigaciones relacionadas con la defensa comunicarse entre sí a través de canales redundantes, incluso en caso de que algunas partes de la red resultasen dañadas en una guerra[5].

Los primeros programas de correo electrónico aparecieron en 1972. En 1985, la Fundación nacional de la ciencia de EE.UU. construyó la red NSFNET con el fin de enlazar seis grandes centros informáticos del país. En los años ochenta dicha red se transfirió a un grupo de universidades llamado MERIT y se fue abriendo paulatinamente a instituciones no académicas y organizaciones no estadounidenses. En 1990, Tim Berners Lee, que trabajaba en el Centro Europeo para la Investigación Nuclear de Ginebra, diseñó el primer navegador y aplicó el concepto de *hipervínculo*, tras lo cual se han ido añadiendo continuamente gran variedad de nuevos servicios y funciones.

Sin embargo, conviene tener en cuenta que el TCP/IP sigue siendo el *protocolo* básico de transmisión de datos en Internet y que todos los servicios dependen de él. Este *protocolo*, cuyo diseño permite una instalación muy sencilla, no depende de ningún sistema operativo ni informático específico.

En Internet, cada ordenador se identifica con una dirección IP numérica única de la forma A.B.C.D, en la que A, B, C y D son números del 0 al 255 (por ejemplo, 194.178.86.66).

Las *redes TCP/IP* se basan en la transmisión de paquetes pequeños de información, cada uno de los cuales contiene la dirección IP del emisor y del destinatario. Estas redes funcionan sin conexiones, lo que significa que, al contrario de lo que sucede con la red telefónica, por ejemplo, no es necesaria una conexión previa entre dos dispositivos para iniciar la comunicación. Esto permite igualmente realizar diversas comunicaciones con interlocutores distintos de forma simultánea.

El *DNS (sistema de nombres de dominio)* es un mecanismo de asignación de nombres a ordenadores identificados con una dirección IP. Dichos nombres presentan la forma <nombre>.dominio de nivel superior, donde <nombre> es una cadena formada por una o varias subcadenas separadas por un punto. El dominio de nivel superior puede ser un dominio genérico (por ejemplo, "com" para páginas web comerciales u "org" para

[3] Los aspectos técnicos descritos en este trabajo se han simplificado enormemente para que los comprendan los profanos en la materia. Para más detalles, véase: *Comunicación de la Comisión al Consejo y al Parlamento Europeo, La organización y gestión de Internet*, Cuestiones de política europea e internacional 1998 - 2000 COM (2000) 202 final, 11 de abril de 2000.
[4] Véase la sentencia Reno contra ACLU de 26 de junio de 1997, Tribunal Supremo de los Estados Unidos, disponible en: www2.epic.org/cda/cda_decision.html.
[5] Véase la sentencia Reno contra ACLU de 26 de junio de 1997.

organizaciones sin ánimo de lucro) o bien un dominio geográfico, como "be" para Bélgica. El *DNS* no es un servicio gratuito y las empresas o las personas que deseen un nombre de dominio deben identificarse. Ciertas herramientas públicas existentes en la Red permiten encontrar el enlace entre el nombre de dominio y la empresa, así como entre la dirección IP y el nombre de dominio. No es necesario un nombre de dominio para conectar un ordenador a Internet. Los nombres de dominio son dinámicos. Un único ordenador conectado a Internet puede tener uno o varios nombres de dominio, o también no tener ninguno, pero un nombre de dominio específico se refiere siempre a una dirección IP determinada.

Actualmente existe una cantidad limitada de direcciones IP. Este número depende de la extensión del campo asignado a la dirección IP en el *protocolo*[6]. En Europa, las direcciones IP se asignan mediante un procedimiento internacional[7] a proveedores de acceso a Internet que las reasignan a sus clientes, ya sean organizaciones o particulares. Gracias a una herramienta de búsqueda de acceso público, como http://www.ripe.net/cgi-bin/whois, se puede identificar al responsable de una determinada reserva de dirección IP. En general, éste será:

- El administrador de una red local con acceso a Internet (por ejemplo, una PYME o un organismo público), que seguramente usará un esquema fijo de direccionamiento IP y mantendrá una lista con la correspondencia entre los ordenadores y las direcciones IP. Si esta persona está utilizando el *protocolo de configuración dinámica del host* (DHCP[8]), el programa *DHCP* dispondrá normalmente de un fichero registro con el número de la tarjeta Ethernet. Este número único en el mundo identifica un ordenador determinado en la red local.

- Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet. En este caso, normalmente el proveedor mantendrá un fichero histórico con la dirección IP asignada, el número de identificación del suscriptor, la fecha, la hora y la duración de la asignación de dirección. Es más, si el usuario de Internet está utilizando una red pública de telecomunicaciones, como un teléfono móvil o fijo, la compañía telefónica registrará el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.

- El titular del nombre de dominio, que podrá ser un nombre de empresa, el nombre de un empleado de una empresa o un particular.

En estos casos, ello significa que, con la asistencia de las terceras partes responsables de la asignación, se puede identificar a un usuario de Internet, es decir, obtener su identidad civil (nombre, dirección, número de teléfono, etc.) por medios razonables.

Un *encaminador* es un dispositivo que proporciona rutas a las *redes TCP/IP*. Esto significa que la ruta TCP/IP es dinámica, pues depende de los fallos o las sobrecargas de algunos *encaminadores* o enlaces. También puede servir como *cortafuegos* entre una

[6] Actualmente se está desarrollando la versión mejorada (Ipv6) del sistema de direccionamiento IP sobre la base de números de 128 bits de longitud.

[7] La Corporación Internet para la asignación de nombres y números (ICANN) es un organismo sin ánimo de lucro fundado para asumir la responsabilidad de la asignación de espacio de dirección IP (http://www.icann.org). En Europa, el espacio de direccionamiento está gestionado por la organización RIPE (Réseaux IP Européens) (http://www.ripe.net). Para más detalles sobre la evolución del proceso de los nombres de dominio de Internet, véase la Comunicación de la Comisión mencionada en la nota al pie 3.

[8] El *Protocolo de configuración dinámica del host* (DHCP) es un *protocolo* de Internet destinado a automatizar la configuración de los ordenadores que usan el TCP/IP. El DHCP puede utilizarse para asignar automáticamente direcciones IP (http://www.dhcp.org).

organización e Internet. En particular, puede garantizar que todas las direcciones que proceden de determinado *proveedor de servicios de Internet* están autorizadas.

Cabe señalar que la velocidad de transmisión es el criterio fundamental de encaminamiento en *redes TCP/IP*. Con información circulando casi a la velocidad de la luz, si en París hay un atasco de la Red puede resultar más eficaz que un paquete TCP/IP enviado de Londres a Madrid pase por Nueva York. Algunas herramientas permiten al usuario de Internet conocer el camino entre dos puntos, aunque en teoría puede cambiar cada segundo e incluso durante la transferencia de una misma página web.

***Protocolos* más sofisticados que emplean el TCP/IP**

A partir del TCP/IP, existen otros *protocolos* capaces de ofrecer determinados servicios. Básicamente, los *protocolos* más utilizados son:

- el HTTP (*protocolo* de transporte de hipertexto), utilizado para navegar,
- el FTP (*protocolo* de transferencia de ficheros), utilizado para transferir ficheros,
- el NNTP (*protocolo* de transferencia de noticias a través de la Red), utilizado para acceder a foros de debate,
- el SMTP (*protocolo* simple de transferencia de correo) y los POP3 (*protocolo* de oficina de correo), utilizados para enviar y recibir correo electrónico.

Jerarquía de niveles y *protocolos* en un proceso de comunicación por Internet

HTTP utilizado para navegar y buscar	SMTP utilizado para enviar correo electrónico	POP3 utilizado para descargar el correo electrónico del servidor de correo al cliente	NNTP utilizado para transferir noticias	FTP utilizado para cargar o descargar ficheros	etc. otros muchos *protocolos* de alto nivel que ya están en uso o se están desarrollando
TCP/IP					
PPP utilizado por los *módems* en líneas telefónicas	X-75 utilizado por adaptadores de terminal en líneas RDSI	*ADSL* utilizada por un *módem ADSL* en líneas de teléfono estándar	ETHERNET utilizado por las tarjetas de redes locales	etc. otros muchos *protocolos* de nivel inferior que ya están en uso o se están desarrollando	

• Estos *protocolos* son necesarios porque el *protocolo* TCP/IP sólo permite transmitir información en masa de un ordenador a otro. El ordenador que ofrece un servicio se denomina SERVIDOR, mientras que el ordenador que utiliza un servicio recibe el nombre de CLIENTE. Para prestar un servicio técnico, tanto el cliente como el servidor han de emplear el mismo *protocolo*, es decir, las mismas normas de comunicación. A menudo se habla de Internet como una red cliente-servidor. Cabe destacar que sea cual sea el servicio utilizado, el *protocolo* TCP/IP se utiliza siempre en todos los servicios anteriormente mencionados. Esto significa que las amenazas a la privacidad relacionadas con el *protocolo* TCP/IP estarán presentes al utilizar cualquier servicio de la Red.

• Con objeto de evitar malentendidos en relación con el significado general de la palabra "servicio", en este texto se empleará el término *protocolo* para designar los *protocolos* HTTP, FTP, NNTP y otros servicios disponibles en Internet.

Un *servidor proxy* es un servidor que actúa como intermediario entre el usuario de Internet y la Red. Funciona como una *caché web* y mejora de forma espectacular la velocidad de visualización de la información (por ejemplo, en la visualización de páginas web). Muchas organizaciones o proveedores importantes de acceso a Internet ya han aplicado esta solución. Cada página, imagen o logotipo descargado desde el exterior por un miembro de una organización se almacena en una caché en el *servidor proxy* y queda automáticamente disponible para los demás miembros de la misma organización.

II. AGENTES PARTICIPANTES EN INTERNET

Cabe señalar que una empresa o un individuo pueden desempeñar distintos papeles en Internet y, por lo tanto, ejecutar simultáneamente distintas operaciones de tratamiento de datos (por ejemplo, registro de conexiones en calidad de operador de telecomunicaciones o almacenamiento de sitios web visitados en calidad de *proveedor de servicios de Internet*), con todo lo que esto implica en la aplicación de principios sobre privacidad.

Operador de telecomunicaciones

En Europa, la infraestructura de telecomunicaciones ha sido, de hecho, monopolio de los operadores tradicionales de telecomunicación. Sin embargo, esta situación está cambiando. Además, a menudo este monopolio se reduce a los cables o las fibras ópticas, mientras que en el caso de las comunicaciones inalámbricas y las nuevas tecnologías, como *WAP*, *UMTS*, etc., está surgiendo la competencia entre los agentes nacionales.

No obstante, el operador tradicional de telecomunicaciones sigue siendo un agente importante, pues es quien se encarga de la comunicación de datos entre el usuario de la Red y el proveedor de acceso a Internet.

Con fines relacionados con la facturación, el operador de telecomunicaciones procesa datos sobre tráfico tales como el número que realiza la llamada y su situación (en el caso de los teléfonos móviles), el número llamado y la fecha, la hora y la duración de la comunicación[9].

Proveedor de acceso a Internet

El proveedor de acceso a Internet proporciona, generalmente sobre la base de un contrato, una conexión TCP/IP a:

- Personas que utilicen un *módem* o un adaptador de terminal (RDSI). En este caso, el abonado recibirá una dirección IP válida durante la conexión que probablemente cambiará la próxima vez que se conecte y se denomina dirección IP dinámica.

Si se trata de una línea *ADSL* (conexión a través de una línea de suscripción asimétrica digital) o de cable de vídeo, la dirección IP será normalmente estática, pues dichas conexiones son permanentes.

[9] El tiempo de tratamiento y almacenamiento de estos datos está sujeto a condiciones jurídicas estrictas, como se explica más adelante.

Para obtener una conexión, una persona[10] ha de firmar un contrato, (la suscripción es gratuita), y dar su nombre, dirección y otros datos personales. Por regla general, el usuario recibirá un nombre de identificación de usuario, que puede ser un seudónimo, y una contraseña, con lo que nadie más podrá utilizar su abono. Aunque sólo sea por motivos de seguridad, los proveedores de acceso a Internet parecen registrar siempre en un fichero, de forma sistemática, la fecha, la hora, la duración y la dirección IP dinámica que se ha dado a un usuario de Internet. En la medida en que es posible vincular el fichero registro a la dirección IP del usuario, esta dirección se ha de considerar un dato de carácter personal.

- Organismos que utilicen una conexión por línea conmutada o, de forma más habitual, una línea arrendada a las oficinas de la empresa. Normalmente, el operador tradicional de telecomunicaciones será quien proporcione la línea. La conexión también se puede establecer vía satélite o mediante un sistema de radio terrestre. El proveedor de acceso a Internet asignará a la empresa direcciones IP y utilizará un *encaminador* para garantizar que éstas se respetan.

Los proveedores de acceso a Internet poseen una o más líneas arrendadas (par trenzado, fibra óptica, enlace vía satélite) conectadas a otros proveedores mayores.

Proveedor de servicios de Internet

El *proveedor de servicios de Internet* ofrece servicios de la Red a empresas y particulares. Es propietario o arrendatario de una conexión TCP/IP permanente y utiliza servidores conectados continuamente a Internet. Por lo general, el proveedor desempeñará el papel de sistema anfitrión (almacenando páginas web en su servidor web) y ofrecerá acceso a foros de debate y a servidores FTP, así como servicios de correo electrónico. Esto implica la utilización por parte de uno o varios servidores de los *protocolos* POP3, SMTP, FTP, NNTP y HTTP.

Las empresas que actúan como proveedores de acceso a Internet a menudo ofrecen también servicios como *proveedores de servicios de Internet*. Por este motivo, el término genérico *proveedor de servicios de Internet* se utiliza en ocasiones para designar tanto a los proveedores de acceso como a los *proveedores de servicios*. No obstante, desde un punto de vista conceptual, los papeles que desempeñan son diferentes. Concretamente, el proveedor de acceso a Internet encaminará, en su calidad de vía de entrada a la Red, todo el tráfico que genere el abonado, mientras que el *proveedor de servicios de Internet* sólo tendrá conocimiento de lo que suceda en sus servidores[11]. En este informe, cuando se utilice el término *proveedor de servicios de Internet* se incluirá normalmente a los proveedores de acceso. El término proveedor de acceso a Internet sólo se empleará cuando sea evidente que se hace referencia exclusivamente al acceso a la Red; en caso contrario se empleará el término genérico *proveedor de servicios de Internet*.

Desde un punto de vista técnico, la presencia de servidores equipados con *protocolos* resultará decisiva en la recopilación de datos personales. En el caso de los servidores HTTP, generalmente se crea sistemáticamente por defecto un fichero registro o un fichero histórico que puede contener todos o algunos de los datos que aparecen en la cabecera de la petición HTTP (charloteo del navegador), además de la dirección IP. El fichero registro es una práctica estándar y todos los servidores lo crean.

[10] Una pequeña empresa también puede firmar un contrato de estas características, pero tales casos no se tendrán en cuenta en este documento.

[11] Este documento no se referirá a los *proveedores de servicios de Internet* como proveedores de contenidos, aunque algunos de ellos los ofrezcan en determinadas circunstancias (por ejemplo, en el caso de los *proveedores de servicios de Internet* que tienen su propio *portal*).

Usuario

El usuario de Internet puede ser un particular que accede a la Red desde su casa, normalmente con una conexión TCP/IP temporal y, por tanto, con una dirección IP dinámica, a través de un *módem* o de un adaptador de terminal (RDSI) o bien con una conexión permanente y una dirección IP estática mediante una línea *ADSL*, televisión por cable, etc. La conexión también se puede realizar a través de un teléfono móvil, aunque suele ser más cara.

Si un abonado proporciona una identidad falsa o utiliza la identidad de otro usuario, dando el nombre de usuario y la contraseña de otra persona, es posible localizar al propietario de la línea a la que se ha asignado una determinada dirección IP comparando esta información con los datos recogidos en el fichero registro del proveedor de acceso a Internet. De hecho, esto es lo que hace la policía para localizar intromisiones delictivas en ordenadores conectados a Internet.

Lo mismo sucede si una persona está utilizando una red local o una intranet.

El usuario puede ser también una organización, una administración pública o una empresa que utiliza Internet no sólo para proporcionar o hallar información, sino también para recoger datos que le sirvan en su trabajo o sus actividades, como procedimientos administrativos, venta de mercancías o prestación de servicios, publicación de guías, anuncios por palabras, envío de cuestionarios, etc.

III. SERVICIOS DISPONIBLES EN INTERNET[12]

Cualquier persona con acceso a Internet puede utilizar gran variedad de métodos de comunicación y de recuperación de la información. Los más habituales son el correo electrónico (capítulo 4), los foros de debate y la charla electrónica (capítulo 6) y la World Wide Web (capítulo 5).

Todos estos métodos se pueden utilizar para transmitir texto y la mayoría de ellos pueden transportar también sonidos, imágenes fijas e imágenes de vídeo animadas. En conjunto, estas herramientas constituyen un medio único, conocido por los usuarios como "ciberespacio", que todas las personas pueden utilizar en cualquier parte del mundo siempre que dispongan de acceso a Internet.

Correo electrónico

El correo electrónico permite a un usuario enviar un mensaje electrónico a otra persona o a un grupo de direcciones. En general, el mensaje se almacena electrónicamente en un servidor hasta que el destinatario comprueba su buzón. A veces avisa de su llegada mediante algún tipo de indicador.

Foros de debate

Los foros de debate se utilizan para compartir información o expresar opiniones sobre temas concretos. Los grupos suelen componerse siempre de los mismos participantes, cuyas aportaciones pueden también ser leídas por otras personas. Existen miles de grupos de este tipo, cada uno de los cuales fomenta el intercambio de información o de opiniones sobre un tema determinado. Cada día se envían alrededor de 100 000 mensajes nuevos.

[12] Se puede consultar una descripción pormenorizada de estos servicios en la sentencia Reno contra ACLU de 26 de junio de 1997.

Salas de charla electrónica ("chat rooms")

Dos o más personas que deseen comunicarse directamente pueden entrar en una sala de charla para iniciar un diálogo en tiempo real escribiendo mensajes que aparecen casi de forma inmediata en las pantallas de los demás.

World Wide Web

El tipo de comunicación más conocido en Internet es la World Wide Web, que permite a los usuarios buscar y recuperar información almacenada en ordenadores remotos. Para expresarlo de una forma sencilla, la Web consiste en una inmensa cantidad de documentos almacenados en distintos ordenadores de todo el mundo.

Navegar por Internet resulta relativamente sencillo. Un usuario puede escribir la dirección de una página que ya conoce o introducir una o más palabras clave en un buscador comercial para encontrar sitios relacionados con un tema que le interese. Normalmente, los usuarios exploran una determinada página web o se trasladan a otra pulsando con el ratón del ordenador en uno de los iconos o enlaces de la página. Desde el punto de vista del lector, la Web se podría comparar a una enorme biblioteca con millones de publicaciones indizadas y fácil acceso o a un centro comercial que se expande de forma irregular para ofrecer bienes y servicios (véase el capítulo 7).

Cualquier persona u organización que disponga de un ordenador conectado a Internet puede "publicar" o recopilar información (véanse los capítulos 6, 7 y 8). Entre quienes publican o recaban datos se encuentran organismos gubernamentales, instituciones educativas, entidades comerciales, grupos de interés y particulares. Pueden ofrecer su información al conjunto de los usuarios de Internet o restringir el acceso a la misma a un grupo seleccionado.

IV. Riesgos para la privacidad[13]

Riesgos para la privacidad inherentes a la utilización del *protocolo* TCP/IP

Dado que Internet se ha considerado desde el principio una red abierta, existen muchas características de los *protocolos* de comunicación que pueden llevar, más por accidente que de forma intencionada, a una invasión de la intimidad de los usuarios de Internet.

En lo que respecta al *protocolo* TCP/IP, hay tres características que parecen constituir una posible invasión de la intimidad.

• La **ruta** que siguen los paquetes TCP/IP es dinámica y se guía por la lógica de conseguir el mejor resultado. En teoría, puede variar durante la descarga de una página web o la transmisión de un correo electrónico, pero en la práctica suele permanecer estática. En telecomunicaciones, los resultados dependen más de la congestión de la Red que de la distancia física existente entre los nodos *(encaminadores).* Esto significa que el camino "más corto" entre dos poblaciones situadas en un mismo país de la UE puede pasar por un país ajeno a la Unión en el que quizá no exista una protección de datos adecuada[14]. El usuario medio de Internet no dispone de medios razonables para modificar este camino, aun en el caso de que conozca la ruta seguida en un determinado momento.

13 La Comisión Nacional de la Informática y de las Libertades (CNIL) francesa cuenta en su sitio web con una sección llamada "Sus huellas" en la que los usuarios de Internet pueden visualizar las huellas que han dejado tras de sí al utilizar Internet. Esta sección se encuentra disponible en francés, inglés y español. Véase www.cnil.fr

14 Para más detalles sobre esta cuestión, véase el capítulo 2.

• La traducción entre el nombre de dominio y la dirección IP numérica se realiza a través de un **servidor DNS** que recibe y puede rastrear todos los nombres de los servidores de Internet con los que el usuario haya intentado contactar. En la práctica, quienes mantienen esos servidores de nombres de dominio suelen ser los proveedores de acceso a Internet, que disponen de capacidad técnica para conocer mucho más que eso, como se verá en los próximos capítulos.

• La orden "**ping**", disponible en todos los sistemas operativos, permite a cualquier persona conectada a Internet saber si un determinado ordenador está encendido y conectado a la Red. Esta orden consiste en escribir las letras PING seguidas de la dirección IP (o el nombre correspondiente) del ordenador. Normalmente, el usuario de éste no sabrá que alguien ha intentado averiguar si estaba conectado a Internet en un determinado momento ni conocerá los motivos por los que lo ha hecho.

Cabría señalar que las conexiones permanentes a Internet realizadas por cable y *ADSL* presentan los mismos riesgos.

Aunque estas operaciones de tratamiento de datos son legítimas y en ocasiones ineludibles para el correcto funcionamiento de Internet, el usuario debería tener conocimiento de ellas y de las medidas de seguridad que puede aplicar.

Riesgos para la privacidad inherentes a la utilización de *protocolos* de alto nivel

Este apartado se centra en tres características que casi siempre están presentes a la hora de emplear el *protocolo* HTTP en los navegadores más utilizados. Conviene subrayar que la combinación de estas características puede acarrear graves consecuencias para la privacidad de los usuarios de Internet.

El *protocolo* HTTP presenta una importancia estratégica en la medida en que es el más utilizado en la Web y puede ofrecer servicios como el correo electrónico y los foros de debate, que hasta ahora se prestaban a través de *protocolos* especializados de alto nivel, como POP3, SMTP o NNTP[15].

El charloteo del navegador

Es un hecho conocido que escribir "http://www.website.org/index.htm" significa "muéstrame la página llamada 'index.htm' en el servidor www.website.org utilizando el *protocolo* HTTP". Se podría creer que sólo la dirección IP de la persona que navega por Internet y el fichero que quiere ver se transmiten al sitio web. Sin embargo, no es así.

La siguiente tabla recoge algunos de los datos que se transmiten de forma sistemática en la cabecera HTTP al realizar una petición HTTP (charloteo del navegador automático) y a los que, por tanto, puede acceder el servidor:

Var. HTTP	*Opera 3.50*	*Netscape 4.0 Fr*	*Explorer 4.0 UK*
GET	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0	GET /index.html HTTP/1.0
User-Agent:	Mozilla/4.0(compatible ; Opera/3.0; Windows 95) 3.50	Mozilla/4.04 [fr] (Win95; I ;Nav)	Mozilla/4.0 (compatible; MSIE 4.01; Windows 95)
Accept:	image/gif, image/x-xbitmap, image/jpeg, /	Image/gif, image/x-xbitmap, image/jpeg	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-

[15] Véase DINANT, Jean-Marc, Law and Technology Convergence in the Data Protection Field? *Electronic threats to personal data and electronic data protection on the Internet*, Proyecto ESPRIT 27028, "Electronic Commerce Legal Issues Platform".

		excel, application/msword, application/vnd.ms-powerpoint, /
Referer:	Where.were.you/doc.htm	Where.were.you/doc.htm
Language:	Fr	fr-be

La definición técnica de estos campos se encuentra en el RFC 1945 para HTTP 1.0 o en el RFC 2068 para HTTP 1.1. Se pueden formular las siguientes observaciones al respecto:

- La primera línea es la única indispensable.
- En la línea "Accept", cada navegador menciona que el usuario de Internet está utilizando Windows 95. Cabría preguntarse por qué. Netscape añade que la versión del navegador es francesa. Cada navegador da la identificación de su nombre, versión y subversión.
- Mientras se describen los formatos aceptados, Microsoft informa a cada sitio de que el ordenador del usuario de Internet tiene instalados Powerpoint, Excel y Word.
- Opera no revela la página remitente.
- Opera no revela el idioma del usuario de Internet, mientras que Netscape dice que es francófono y Microsoft, además, revela que es belga francófono.

Hipervínculos invisibles

Los *hipervínculos* constituyen el valor añadido de Internet. Gracias a ellos se puede navegar de un continente a otro con hacer un simple clic con el ratón. Lo que el usuario corriente no ve es que los programas clásicos de navegación permiten incluir en el código HTML de la página una petición HTTP de descargar imágenes. No es necesario que esas imágenes se encuentren en el mismo servidor que ha recibido la petición de presentar una determinada página web.

En este caso, la variable HTTP_REFERER contiene la referencia de la página remitente, es decir, la página principal en la que se localizarán las imágenes. En otras palabras: si un sitio web incluye en su página en HTML un vínculo invisible con una imagen situada en el sitio web de una empresa de cibermarketing, ésta conocerá la página remitente antes de enviar la *pancarta* publicitaria. Cuando se realiza una búsqueda con un motor de búsqueda, el nombre de la página web incluye las palabras clave que se han introducido.

Cookies

Las *cookies* son datos que se pueden almacenar en ficheros de texto en el disco duro del usuario y de los que el sitio web puede conservar una copia. Forman parte del tráfico HTTP, por lo que se pueden transportar sin problemas con el tráfico IP.

Las *cookies* residen en el disco duro del usuario y recogen información sobre él que el sitio web que las depositó puede recuperar, o que alguien que conozca el formato de los datos de la página web puede leer. Una *cookie* puede contener todo tipo de información que el sitio web quiera incluir en ella: páginas visitadas, anuncios consultados, número de identificación del usuario, etc.[16]. En algunas ocasiones, pueden resultar útiles para ofrecer un determinado servicio a través de Internet o para simplificar la navegación del usuario. Por ejemplo, algunos sitios web utilizan *cookies* para identificar a sus usuarios

[16] Véase el libro de HAGEL III, J. y SINGER, M., *Net Worth: the emerging role of the informediary in the race for customer information,* Harvard Business School Press, 1999, p. 275.

cada vez que éstos los vuelven a visitar, de modo que no necesitan registrarse cada vez que quieren consultar las novedades.

La SET-COOKIE se instala en la cabecera de la respuesta HTTP[17], concretamente en *hipervínculos* invisibles. Para una duración determinada[18], la *cookie* se almacena en el disco duro del usuario de Internet y se vuelve a enviar al sitio web que la originó o a otros sitios pertenecientes al mismo subdominio. Este reenvío se efectuará a través de un campo COOKIE que formará parte del charloteo del navegador ya descrito.

Utilizando conjuntamente el charloteo del navegador e *hipervínculos* invisibles, una empresa de cibermarketing puede, por defecto, conocer todas las palabras clave introducidas por un usuario de Internet en el motor de búsqueda en el que se anuncia la empresa, así como el ordenador, el sistema operativo, la marca de navegador del usuario de Internet, su dirección IP y la hora y la duración de las sesiones HTTP. La combinación de estos datos sin procesar con otros que ya posea la empresa permite la deducción de nueva información, tal como[19]:

1. El país donde vive el usuario de Internet.
2. El dominio de Internet al que pertenece.
3. El sector de actividad de la empresa donde trabaja.
4. La facturación y el volumen de la empresa donde trabaja.
5. La función y el puesto del usuario de Internet dentro de dicha empresa.
6. El proveedor de acceso a Internet.
7. El tipo de sitios web que actualmente visita.

La *cookie* permite el envío sistemático de un identificador permanente y único con cada petición de información, mientras que la dirección IP resulta ser un identificador relativamente débil, pues puede quedar oculto por proxies, y poco fiable, debido a su carácter dinámico en el caso de los usuarios que acceden a Internet con un *módem*. Muchas empresas de cibermarketing han adoptado este proceso invisible de elaboración de perfiles[20].

Riesgos para la privacidad relacionados con la aplicación del *protocolo* HTTP en los navegadores habituales

La combinación de charloteo del navegador, *hipervínculos* invisibles y *cookies* proporciona los medios necesarios para elaborar un perfil invisible de cada usuario de Internet que utiliza un navegador instalado por defecto. Este perfil no está "en sí mismo" vinculado al *protocolo* HTTP, como ha definido el *W3C*[21]. Además, la definición del

[17] Técnicamente hablando, también es posible implementar *cookies* en *JavaScript* o en los campos <META-HTTP EQUIV> ubicados en el código HTML.

[18] Las *cookies* sin duración fija se llaman "*cookies* de sesión" y desaparecen cuando el navegador o la conexión se cierran.

[19] GAUTHRONET, Serge , "On-line services and data protection and the protection of privacy", Comisión Europea, 1998, pp. 31 y 92, disponible en: http://europa.eu.int/comm/dg15/en/media/dataprot/studies/servint.htm

[20] Sólo con DoubleClick, unos 26 millones de usuarios de Internet en marzo de 1997 (GAUTHRONET, *op. cit*., p. 86) y más de un millardo de *pancartas* publicitarias descargadas cada mes fuera de los Estados Unidos (*ibid*., p. 96). En la actualidad, cada día se envían más de 500 000 000 *pancartas* publicitarias por empresa de cibermarketing. Véase http://www.doubleclick.net/company_info/investor_relations/financials/analyst_metrics.htm.

[21] El *World Wide Web Consortium* (W3C) es una organización sin ánimo de lucro albergada por el Inria (Francia), el Instituto tecnológico de Massachusetts (EE.UU.) y la Universidad de Keio (Japón). Entre sus miembros destacan Microsoft, AOL, Netscape y el "Center for Democracy and Technology".

protocolo HTTP 1.1 ha llamado explícitamente la atención de la industria sobre posibles cuestiones relacionadas con la privacidad inherentes a la utilización del *protocolo* HTTP[22]:

– *"La descripción de las capacidades del agente usuario en cada petición puede resultar muy ineficaz (dado que sólo un pequeño porcentaje de respuestas tienen representaciones múltiples) y una posible violación de su intimidad"* [página 68].
– *"El envío de una cabecera Accept-Language con las preferencias lingüísticas completas del usuario en cada petición puede ir en contra de sus expectativas de protección de la privacidad"* [página 98].
– *"El cliente NO DEBERÍA enviar el campo de cabecera From[23] sin el consentimiento del usuario, pues ello puede ser contrario a los intereses de intimidad del mismo o a la política de seguridad del sitio web. Es muy recomendable que el usuario pueda prohibir, autorizar y modificar el valor de este campo en todo momento antes de una petición"* [página 118].
– *"A menudo, los clientes HTTP tienen acceso a grandes cantidades de datos personales, como el nombre del usuario, su situación y dirección postal, su contraseña, sus claves de* encriptación*, etc., y DEBERÍAN ser extremadamente prudentes para evitar cualquier fuga involuntaria de esta información a otras fuentes a través del* protocolo *HTTP. Se recomienda encarecidamente que se establezca un interfaz para que el usuario pueda controlar la divulgación de esta información y que los diseñadores y desarrolladores presten una atención especial a esta cuestión. La historia demuestra que errores de este tipo provocan a menudo graves problemas de seguridad o de intimidad y que suelen constituir una publicidad extremadamente perjudicial para la empresa responsable"* [página 143][24].

V. Cuestiones económicas

El crecimiento de Internet en los últimos años ha sido espectacular. Entre 1981 y 1996, el número de ordenadores que almacenan la información y proporcionan las comunicaciones ("host") aumentó de unos 300 a cerca de 9 400 000. En torno al 60 % de ellos se encuentran en los Estados Unidos. En 1996 unos 40 millones de personas eran usuarios de Internet; se espera llegar a unos 200 millones[25] para 2000 y se prevé que en 2005 la mitad de la población europea esté conectada a la Red[26].

En muchos países europeos la suscripción de los particulares a Internet es gratuita, pero el abonado tiene que pagar al operador de telecomunicaciones por la línea. El proveedor de acceso o el *proveedor de servicios de Internet* obtendrá una remuneración del operador de telecomunicaciones en forma de una prima de retroconexión que dependerá de la duración de la llamada local realizada por el abonado a Internet. Esto significa que, aunque no deba pagar por la suscripción a Internet, el usuario ha de hacer frente a los gastos de las líneas telefónicas utilizadas, lo que beneficiará tanto a los proveedores de acceso y de servicios de Internet como a los operadores de telecomunicación.

Los fabricantes de software también se beneficiarán de la utilización de Internet, pues aunque ofrezcan sus productos al consumidor de forma gratuita (software gratuito,

---

(http://www.w3.org/Consortium/Member/List). El W3C genera normas no vinculantes pero aplicables de hecho destinadas a garantizar la interoperabilidad de los ordenadores en Internet.
[22] http://www.w3.org/Protocols/rfc2068/rfc2068. La paginación entre corchetes corresponde a la del *W3C*.
[23] El campo de cabecera "From" se utiliza para designar la página remitente.
[24] La palabra "privacidad" aparece 18 veces en el RFC 2068.
[25] Véase la sentencia Reno contra ACLU de 26 de junio de 1997.
[26] Comunicado de prensa de la Comisión Europea, *Commission welcomes new legal framework to guarantee security of electronic signatures*, 30 de noviembre de 1999.

navegadores, etc.), perciben una remuneración por el uso que los servidores de sitios web hacen de sus programas.

La venta directa es una de las actividades más lucrativas de la Red. Las empresas de cibermarketing instalan *pancartas* publicitarias en páginas web, a menudo de tal forma que la recopilación de datos personales resulta invisible para el titular de los datos. El uso de enlaces invisibles, junto con el charloteo del navegador y las *cookies*, permite que empresas de venta desconocidas elaboren perfiles individualizados de los usuarios de Internet. Una sola empresa de cibermarketing podría vender aproximadamente medio millardo de *pancartas* publicitarias al día. Las empresas de venta directa financian muchos motores de búsqueda.

Instalando *hipervínculos* invisibles a empresas de cibermarketing en sus propias páginas web, los sitios web más visitados (especialmente los motores de búsqueda) enviarán una orden a navegadores como Netscape e Internet Explorer para que abran una conexión independiente HTTP con el servidor HTTP de la empresa de cibermarketing. Como ya se ha explicado, mientras gestiona la petición HTTP, el navegador comunicará automáticamente varios datos, a saber: la dirección IP, la página remitente (en el caso de un motor de búsqueda, esta variable contiene las palabras clave introducidas por el usuario), la marca, la versión y el idioma del navegador (por ejemplo, Internet Explorer 4.02, neerlandés) y el tipo y el sistema operativo utilizados (Windows 2000, Linux 2.2.5, Mac OS 8.6, etc.), así como la *cookie* de identificación (como UserId=342ER432), que tal vez la empresa de cibermarketing ya haya incorporado con *hipervínculos* invisibles previos.

Normalmente, el usuario medio de Internet ignora que muchas de las *pancartas* que ve tras introducir un URL (localizador de recursos uniforme) no proceden del sitio web que está visitando. Tampoco sabe que al descargar una *pancarta* publicitaria su navegador transmitirá sistemáticamente una serie de datos únicos, como la identidad, la dirección IP y el URL completo de la página web en la que se encuentra, incluidas también las palabras clave tecleadas en motores de búsqueda y el nombre de los artículos de prensa que está leyendo en línea. Todos esos datos pueden combinarse para determinar el perfil general de un ciudadano que navega de una página a otra, gracias a la identidad única almacenada en la *cookie*.

Se considera que la recopilación de información relativa al usuario en entornos en línea es una práctica de importancia económica y estratégica. Las siguientes líneas, extraídas de una famosa publicación americana[27], ilustran esta idea: *Son demasiadas las empresas, incluidas muchas compañías punteras que están surgiendo en Internet, que no se han centrado lo suficiente en el valor de los perfiles de los clientes. Quien posea los derechos sobre los perfiles de los clientes en línea será quien determine los ganadores y los perdedores de esta nueva era.*

Conviene mencionar que la recopilación de datos de usuarios de Internet suele ser gratuita para la empresa, pues a menudo son los propios consumidores quienes los proporcionan a través, por ejemplo, de formularios. Los sitios web recurren habitualmente a programas de fidelidad, como juegos, cuestionarios o boletines informativos, que obligan al visitante de la página a comunicar datos personales.

Algunos casos recientes confirman el valor creciente que las empresas otorgan a los perfiles de los consumidores. Las listas de clientes se venden o comparten, principalmente a través de la fusión de compañías de tecnología de la información que de este modo aumentan la cantidad de datos y perfiles a su disposición.

[27] Véase el libro *Net Worth (op. cit.)*, página xiii (prefacio).

Finalmente, se darán adquisiciones basadas en datos del consumidor en las que éstos sean los activos primarios objeto de la compra. (…) Actualmente, los datos del consumidor constituyen, de muchas formas, la moneda de cambio del comercio electrónico. Dichos consumidores son clientes valiosos, pues han demostrado que compran y han comprado a la competencia. (…) Los nombres existentes en una base de datos permiten a las empresas importantes ahorros situados en torno a 100 USD por cliente[28] *en publicidad destinada a conseguir nuevos clientes.*

Los datos de los clientes también se ponen a la venta cuando quiebran las empresas de Internet. Recientemente, una empresa de juguetes ha incluido en su liquidación la venta de los perfiles de sus clientes. Estos perfiles se recopilaron de acuerdo con una política de privacidad consistente en no comunicar nunca dicha información a terceros sin el consentimiento expreso del cliente. Los perfiles contenían el nombre, la dirección, datos de facturación, información sobre el comportamiento de compra y el perfil familiar, con los nombres y las fechas de nacimiento de los hijos.

El 8 de agosto de 2000, TRUSTe, que había aprobado la política de privacidad de la empresa, anunció que había presentado una reclamación ante el Tribunal de quiebras de los Estados Unidos en contra del consentimiento de la Comisión federal de comercio a las condiciones de liquidación de los activos de la empresa[29].

Una política completa de protección de la privacidad debe tener en cuenta el equilibrio entre los intereses económicos y los derechos humanos. Quedan por resolver dos grandes cuestiones:

- Se ha recabado en Internet gran cantidad de datos personales sobre usuarios de la Red sin el conocimiento y/o el consentimiento previo de sus titulares, debido principalmente a los efectos secundarios invisibles de la tecnología Internet. Es probable que en los próximos años aumente el intercambio de datos personales con fines lucrativos[30], pero ¿hasta dónde llegará el usuario de Internet en esta práctica? ¿Qué tipo de información personal puede compartir el propio titular, por cuánto tiempo y en qué circunstancias?
- Si la financiación de determinados sitios web, como los motores de búsqueda, se realiza principalmente con cargo a la industria del cibermarketing, puede existir la tentación de recurrir a elaborar perfiles personalizados para garantizar que servicios hasta entonces gratuitos excluyan a quienes no dispongan de un nivel suficiente de ingresos, no hayan respondido a cientos de *pancartas* publicitarias o deseen proteger su privacidad.

VI. Conclusiones

- Internet se concibió como una red mundial abierta (www) a través de la cual se podría compartir información. Sin embargo, es necesario encontrar un equilibrio entre el "carácter abierto" de Internet y la protección de los datos personales de los usuarios de la Red.
- Con frecuencia se recaba en Internet gran cantidad de información sobre los usuarios de la Red sin que ellos lo sepan. Es necesario tratar esta falta de transparencia con los usuarios de Internet, con el fin de alcanzar un grado aceptable de protección del consumidor y de sus datos personales.

[28] Citado de M. HALPERN y HARMON, *E-mergers trigger privacy worries* de Deborah KONG, http://www.mercurycenter.com/svtech/news/indepth/docs/consum012400.htm.
[29] http://www.truste.org/users/users_investigations.html.
[30] Véase, por ejemplo, el debate sobre los informediarios en el capítulo 9.

- Los *protocolos* son medios técnicos que determinan la forma en que se recogen y se tratan los datos. Los navegadores y el software desempeñan también un papel importante. En algunos casos están dotados de un identificador que permite relacionar al usuario de Internet con sus actividades en la Red. Por lo tanto, corresponde a los agentes que intervienen en su diseño y su desarrollo ofrecer al usuario productos que respeten la privacidad. En ese sentido, conviene señalar que el artículo 14 del proyecto de Directiva sobre telecomunicaciones de 12 de julio de 2000 afirma que, cuando sea preciso, la Comisión deberá adoptar medidas destinadas a asegurar que los equipos técnicos incorporan las garantías necesarias para proteger la información de carácter personal y la privacidad de los usuarios y abonados.

CAPÍTULO 3: APLICACIÓN DE LA LEGISLACIÓN RELATIVA A LA PROTECCIÓN DE DATOS

I. Cuestiones jurídicas generales

El análisis jurídico de los distintos fenómenos existentes que se presenta en los próximos capítulos se basa en que las dos Directivas sobre protección de datos (Directiva 95/46/CE y Directiva 97/66/CE) se aplican en principio a los datos de carácter personal tratados en Internet[31].

Todas las consideraciones jurídicas que aparecen en este documento se basan en la interpretación de estas Directivas, así como en los documentos adoptados por el Grupo de Trabajo y, cuando así se indica, en la jurisprudencia del Tribunal Europeo de Derechos Humanos.

Datos personales en Internet

Como ya se ha mencionado en este documento, los proveedores de acceso a Internet y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP, pues registran sistemáticamente en un fichero la fecha, la hora, la duración y la dirección IP dinámica asignada al usuario de Internet. Lo mismo puede decirse de los *proveedores de servicios de Internet* que mantienen un fichero registro en el servidor HTTP. En estos casos, no cabe duda de que se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 2 de la Directiva[32].

En otros casos, un tercero puede llegar a averiguar la dirección IP dinámica de un usuario pero no ser capaz de relacionarla con otros datos que le permitan identificarlo. Obviamente, resulta más sencillo identificar a los usuarios de Internet que utilizan direcciones IP estáticas.

Sin embargo, en muchos casos existe la posibilidad de relacionar la dirección IP del usuario con otros datos de carácter personal, de acceso público o no, que permitan identificarlo, especialmente si se utilizan medios invisibles de tratamiento para recoger información adicional sobre el usuario, tales como *cookies* con un identificador único o sistemas modernos de *minería de datos* unidos a bases de datos con información sobre usuarios de Internet que permite su identificación.

Así pues, aunque no siempre sea posible para todos los agentes de Internet identificar a un usuario a partir de datos tratados en la Red, este documento parte de la idea de que la posibilidad de identificar a un usuario de Internet existe en muchos casos y, por lo tanto, en Internet se tratan grandes cantidades de información personal para la cual son de aplicación las Directivas sobre protección de datos.

Aplicación de las Directivas

Como ya ha afirmado con anterioridad el Grupo de Trabajo, la Directiva general 95/46/CE sobre protección de datos se aplica a todo tratamiento de datos de carácter personal que entre en su ámbito de aplicación, independientemente de los medios técnicos utilizados. Por consiguiente, el tratamiento de datos personales en Internet ha de

[31] Véase WP 16, Documento de trabajo: *Tratamiento de datos personales en Internet*, aprobado por el Grupo de Trabajo el 23 de febrero de 1999, 5013/99/ES/final.

[32] Véase también el considerando 26 del preámbulo de la Directiva.

considerarse a la luz de esta Directiva[33]. Así pues, la Directiva general resulta aplicable en todos los casos y a todos los agentes mencionados en la primera parte de este capítulo (descripción técnica).

La Directiva específica 97/66/CE relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las telecomunicaciones detalla y completa la Directiva general 95/46/CE, pues fija disposiciones técnicas y jurídicas específicas. La Directiva 97/66/CE se aplica al tratamiento de datos de carácter personal en relación con la prestación de servicios públicos de telecomunicación en redes públicas de telecomunicaciones dentro de la Comunidad. Los servicios de Internet son servicios de telecomunicaciones, por lo que Internet queda incluido en el sector de las telecomunicaciones.

La Directiva 95/46/CE se aplica a todas las cuestiones que no quedan específicamente cubiertas por la Directiva 97/66/CE, tales como las obligaciones relativas al responsable y los derechos individuales, o los servicios de telecomunicaciones no públicos[34]. Los datos personales que el usuario de Internet proporciona de forma voluntaria durante su conexión a la Red corresponderán siempre al ámbito de aplicación de esta Directiva.

La tabla siguiente intenta definir los casos en que la Directiva específica 97/66/CE es de aplicación y aquéllos en que lo es la Directiva 95/46/CE, así como establecer los principios más pertinentes. Sin embargo, se ha de tener en cuenta que cuando los agentes desempeñan varios papeles al mismo tiempo se producirá cierta superposición.

Agente	**Función**	**Posible tratamiento de datos personales**	**Preceptos pertinentes de la Directiva de telecomunicaciones**
Proveedor de telecomunicaciones Ej.: AT&T	- Conectar al usuario de Internet con el *proveedor de servicios de Internet*	- Registro de conexiones entre el usuario de Internet y el *proveedor de servicios de Internet* -Transferencia de la *identificación de la línea llamante* del usuario al *proveedor de servicios de Internet*	- Directiva de telecomunicaciones, y en especial confidencialidad de las comunicaciones y de los datos sobre facturación y tráfico y presentación y restricción de la identificación de la línea llamante y de la línea conectada.
Proveedor de servicios de Internet[35] Ej.: World Online	- Prestar el servicio de Internet solicitado - Transferir la petición del usuario de Internet al *servidor proxy* (caché) - Transferir la petición del usuario de Internet al sitio web - Transferir la respuesta del *servidor proxy* al usuario de Internet - Transferir la respuesta del sitio web al usuario de Internet	- Registro de las *identificaciones de líneas de llamada* entrantes - Asignación de dirección IP a una sesión - Posibilidad de almacenar listas de visitas a los sitios web clasificadas por dirección IP - Intercambio de datos con los sitios web solicitados - Registro de las sesiones (hora de inicio y fin de la sesión y cantidades de datos transferidos) - *Minería de datos* de cabeceras y contenido.	- Directiva de telecomunicaciones, y en especial confidencialidad de las comunicaciones y de los datos de facturación y tráfico.

[33] En este documento, la expresión "la Directiva" se referirá a la Directiva 95/46/CE.
[34] Véase el considerando 11 de la Directiva 97/66/CE.
[35] En principio, el término *proveedor de servicios de Internet*, tal y como se emplea en este documento, se refiere también a los proveedores de acceso a Internet (véase la definición en el glosario). Este documento

Servicios de portal Ej.: Yahoo, AOL, Macropolis	- Seleccionar el suministro de información - Ofrecer información (proveedor de contenidos) y, en ocasiones, bienes y servicios	- Registro de las peticiones a los sitios que están tras el *portal* - Posible registro de las visitas realizadas al sitio - Registro de páginas remitentes y palabras clave introducidas (datos de charloteo) - Envío de *cookies* al disco duro del usuario de Internet - Elaboración de perfiles	- Directiva de telecomunicaciones (aplicable al *proveedor de servicios de Internet* que aloja el *portal*).
Página inicial / sitio web muy visitado Ej.: www.coe.int	- Ofrecer información (proveedor de contenidos) y, en ocasiones, bienes y servicios	- Posible registro de visitas realizadas al sitio - Registro de páginas remitentes y palabras clave introducidas (datos de charloteo) - Envío de *cookies* al disco duro del usuario de Internet - Elaboración de perfiles	
Proveedores de servicios adicionales Ej.: Nedstat, Doubleclick, Banners	- Personalizar páginas web	- Elaboración de perfiles (fusionando las *series de clics* de varios sitios web)	- No siempre constituye un servicio de telecomunicación, por lo que la Directiva de telecomunicaciones sólo se aplica en algunos casos.
Proveedores de *encaminadores* y de líneas de conexión (con frecuencia propiedad de los proveedores de telecomunicaciones)	- Conectar a los *proveedores de servicios de Internet*	- Direccionamiento de datos de un usuario de Internet al sitio web IP - Riesgo de interceptación ilegal	- Directiva de telecomunicaciones, y en especial seguridad y confidencialidad de las comunicaciones.

Es evidente que la clave para decidir si las dos Directivas son o no aplicables radica en determinar si el servicio prestado puede considerarse un "servicio de telecomunicación" conforme a la definición recogida en la letra d) del artículo 2 de la Directiva 97/66/CE: *la transmisión y el envío de señales a través de redes de telecomunicación.*

Si la Directiva específica sobre telecomunicaciones es de aplicación, se han de adoptar las normas específicas de ésta.

Proveedor de telecomunicaciones

No cabe duda de que la conexión de un usuario de Internet a un *proveedor de servicios de Internet* que preste servicios de Internet y encamine las solicitudes y las respuestas de los usuarios a los servidores de sitios web y viceversa constituye un servicio de telecomunicaciones. Por lo tanto, la Directiva 97/66/CE es aplicable a los proveedores de telecomunicaciones, a los *proveedores de servicios de Internet* y a los proveedores de líneas y de *encaminadores* destinados al tráfico de Internet.

sólo se referirá a proveedores de acceso a Internet cuando aborde cuestiones que se refieran exclusivamente a ellos.

Proveedores de servicios de Internet (incluidos los proveedores de acceso a Internet)

Lo mismo puede decirse de los *proveedores de servicios de Internet*: no cabe duda de que la Directiva específica sobre telecomunicaciones es también aplicable a sus actividades.

Un caso interesante es el de las instituciones o personas que tienen acceso directo a Internet sin necesidad de recurrir a un *proveedor de servicios de Internet*. Estas instituciones actúan en realidad como *proveedores de servicios de Internet* que conectan su propia red privada a Internet.

El artículo 3 de la Directiva 97/66/CE define su ámbito de aplicación especificando que afecta a los servicios públicos de telecomunicación en las redes públicas de telecomunicación en la Comunidad. En el caso mencionado no se trata de una red pública, sino de una red privada para un grupo determinado de usuarios. Así pues, se puede concluir que, pese a responder a la definición de servicios de telecomunicación, esos servicios no se pueden considerar públicos y, por lo tanto, no corresponden al ámbito de aplicación de la Directiva 97/66/CE.

Es importante señalar que, en tales casos, lo dispuesto en la Directiva específica podría aplicarse de nuevo si la información se enviase fuera de la red privada.

Obviamente, la Directiva general sobre protección de datos resulta plenamente aplicable en estos casos.

Sitios web muy visitados

En general, un sitio web está alojado en un *proveedor de servicios de Internet* (por ejemplo, el sitio web del Consejo de Europa), lo que significa que su responsable arrienda a un *proveedor de servicios de Internet* cierta capacidad de almacenamiento para instalar su sitio web y ponerlo a disposición del público. Asimismo, implica que el *proveedor de servicios de Internet* responde a las peticiones de páginas web de los usuarios de Internet en nombre del Consejo de Europa.

En consecuencia, la persona que "administra" el sitio web (en este caso, el Consejo de Europa) sólo decide sobre la información que se publicará en el sitio web, pero no realiza ningún tipo de operación *que conlleve la transmisión o el encaminamiento de señales en las redes de telecomunicación.*

En el caso de los sitios web en los que pueden solicitarse bienes o servicios, quien los suministre será el responsable del sitio. Sin embargo, cuando se trate de servicios de telecomunicación como tales, normalmente los suministrará el *proveedor de servicios de Internet*, y no el responsable del sitio web.

Por lo tanto se puede afirmar que los sitios web contratan servicios de telecomunicación (transmisión) del *proveedor de servicios de Internet*, pero que no realizan ningún servicio ellos mismos. La Directiva 97/66/CE es aplicable al *proveedor de servicios de Internet* como tal, pero no a los sitios web, que corresponden al ámbito de aplicación de la Directiva general.

Servicios de portal

Un *portal* ofrece una presentación ordenada de enlaces. El usuario de Internet puede visitar fácilmente determinados sitios web de otros proveedores de contenidos a través del *portal* visitado.
Los *portales* están alojados en *proveedores de servicios de Internet*. En algunos casos, el *portal* pertenece al *proveedor de servicios,* como sucede con Worldonline.nl; en otros, el

proveedor de servicios de Internet aloja el *portal* para un tercero que proporciona los contenidos.

En ambos casos, quien presta el servicio de telecomunicación es el *proveedor de servicios de Internet*, tal como se define en el artículo 2 de la Directiva 97/66/CE, y es a él a quien se aplica dicha Directiva, y no al proveedor de contenidos.

Servicios adicionales

El proveedor de servicios adicionales no siempre queda dentro del ámbito de aplicación de la Directiva sobre protección de la intimidad y telecomunicaciones.

Algunos de estos proveedores de servicios, como Nedstat, tratan datos recabados de sitios web y los vuelven a vender a los propietarios de los sitios. Los datos que tratan proceden de Internet, pero en principio su actividad no implica *la transmisión o el encaminamiento de señales en redes de telecomunicación*. Por lo tanto, no desempeñan un papel fundamental en el proceso de telecomunicación entre el usuario de Internet y el sitio web. Si los datos que procesan sólo consisten en datos agregados no identificables, se podría incluso decir que no corresponden al ámbito de aplicación de la Directiva general, pues no entra en juego ningún dato de carácter personal.

Agentes como Doubleclick, Engage o Globaltrash colocan anuncios en páginas solicitadas. Normalmente existe un contrato entre estos anunciantes y el *proveedor de servicios de Internet* que aloja las páginas web en las que se muestra la publicidad.

Técnicamente, cada vez que se accede a un sitio web éste contacta mediante un *hipervínculo* automático con el anunciante para que coloque *pancartas* en las páginas solicitadas.

Por otra parte, el anunciante puede colocar ficheros *cookie* en el disco duro del ordenador del usuario de Internet con objeto de elaborar perfiles de los visitantes del sitio y personalizar así las *pancartas* que aparecen en la página web[36].

No está claro si las actividades básicas de Doubleclick, Engage y otros anunciantes pueden considerarse servicios de telecomunicación o no. Parece ser que no transmiten ni encaminan señales de acuerdo con la definición del artículo 2 de la Directiva de telecomunicaciones, sino que ofrecen contenidos informativos que se colocan en las páginas web solicitadas utilizando las redes y las infraestructuras de telecomunicación existentes.

En cualquier caso, éste es un buen ejemplo de una situación en la que resulta difícil aplicar la definición vigente de servicios de telecomunicación a servicios relacionados con Internet.

II. Revisión de la Directiva de telecomunicaciones: definición de "servicios de comunicación electrónica"

La Comisión Europea anunció en una Comunicación de 1999[37] su intención de llevar a cabo una revisión general del marco jurídico vigente aplicable a las telecomunicaciones en Europa. En el transcurso de esta revisión general se examinará y actualizará también la Directiva vigente sobre tratamiento de datos personales y protección de la intimidad en el sector de las telecomunicaciones.

[36] En la página 275 del libro *Net Worth (op. cit.)* se menciona: "Dado que las *cookies* se pueden utilizar también para relacionar hábitos y preferencias de navegación, se está extendiendo su uso para dirigir los anuncios a usuarios específicos. Doubleclick, Globaltrash y ADSmart son ejemplos de empresas que utilizan *cookies* para adaptar los anuncios a los consumidores en los sitios web programados".

[37] Documento COM (1999) 539.

El Grupo de Trabajo del artículo 29 ya publicó algunas reflexiones relacionadas con esta revisión en su dictamen 2/2000, presentado por el Grupo operativo sobre Internet y aprobado el 3 de febrero de 2000[38].
El texto de la Comunicación de la Comisión Europea destacaba que la revisión prevista prestaría especial atención a la terminología utilizada en la Directiva 97/66/CE, con el fin de aclarar que los nuevos servicios y tecnologías quedan cubiertos por esta Directiva, con lo que se evitarán posibles ambigüedades y se facilitará la aplicación coherente de los principios sobre protección de datos. En su dictamen 2/2000, el Grupo de Trabajo juzgó favorablemente la revisión de la terminología con este fin.
La Comisión publicó la propuesta de Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas[39]. En su comunicado de prensa[40], la institución subraya que uno de los objetivos del nuevo paquete es garantizar la protección del derecho a la privacidad en Internet.

Esta propuesta ya no habla de "servicios de telecomunicación", sino de "servicios de comunicaciones electrónicas". La exposición de motivos de la propuesta afirma que este cambio era necesario para adaptar la terminología a la propuesta de Directiva y establecer un marco común de las redes y los servicios de comunicaciones electrónicas[41].

La expresión "servicios de comunicaciones electrónicas" no se define en la propuesta de Directiva de intimidad y telecomunicaciones, sino en la letra b) del artículo 2 de la propuesta de Directiva, que establece un marco común de las redes y los servicios de comunicaciones electrónicas.

La nueva definición reza: *(Se entenderá por) "servicio de comunicaciones electrónicas", el prestado contra remuneración que consiste, en su totalidad o principalmente, en la transmisión y encaminamiento de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante el uso de redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos."*

De hecho, la nueva definición se basa en la misma idea que la anterior (la transmisión y el encaminamiento de señales en servicios de comunicación electrónica), pero contiene una lista de servicios incluidos en la definición y excluidos de ella que resulta muy útil, pues aclara los debates esbozados en el apartado anterior.

De esta lista incorporada a la nueva definición se puede concluir que los servidores de contenidos transmitidos a través de redes y servicios de comunicación electrónica no pertenecerán al ámbito de aplicación de la Directiva revisada sobre intimidad y telecomunicaciones. Así se confirma en el preámbulo de la propuesta de Directiva, que establece un marco común para las redes y los servicios de comunicación electrónica (séptimo considerando) en el que se afirma que *es necesario separar la regulación de la transmisión de la regulación de los contenidos.* Sin embargo, se acepta que esta separación no debe pasar por alto las relaciones existentes entre ellas.

La consecuencia más importante de esta separación es que servicios adicionales, tales como DoubleClick o los que suministran contenidos a un *portal* o a un sitio web (sin alojarlos), no quedan cubiertos por esta Directiva, sino simplemente por la Directiva

[38] Dictamen 2/2000 sobre la revisión general de la normativa de telecomunicaciones, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, WP 29, 5009/00/ES/final.
[39] Documento COM (2000) 385.
[40] La Comisión propone una revisión de la normativa sobre comunicación electrónica, Bruselas, 12 de julio de 2000, IP/00/749.
[41] COM (2000) 393.

general. También significa que los *proveedores de servicios de Internet* quedan dentro del ámbito de aplicación de la Directiva específica siempre que actúen como proveedores de acceso y ofrezcan conexión a Internet, pero que cuando actúen como proveedores de contenidos sólo se les aplicará la Directiva general[42].

La ventaja que ofrece una división clara entre las normas referentes a los contenidos y las relativas a la transmisión es la claridad. Sin embargo, en la práctica resultará más difícil aplicar dicha separación. Pensemos, por ejemplo, en el caso de un *proveedor de servicios de Internet* que ofrezca también contenidos alojando su propio *portal*. Este *proveedor* deberá aplicar la Directiva general a todas sus actividades y la Directiva específica (que impone obligaciones específicas) a las actividades en las que actúa como proveedor de acceso.

Otro aspecto interesante de la nueva definición de "servicios de comunicaciones electrónicas" es la referencia a la remuneración por el servicio. Ni en el preámbulo ni en la exposición de motivos se menciona la inclusión de este término y tampoco se orienta sobre cómo interpretarlo. Una posible interpretación sería que los proveedores de acceso gratuito a Internet quedarían fuera del ámbito de aplicación de la Directiva revisada sobre intimidad y telecomunicaciones, ya que no perciben remuneración alguna, o al menos no financiera, de los usuarios de Internet.

Sin embargo, esta interpretación no es correcta, pues en la jurisprudencia del Tribunal Europeo de Justicia se menciona claramente que, en relación con los servicios en el sentido del artículo 50 (antiguo artículo 60) del Tratado CE[43], no es necesario que la remuneración vaya a cargo del beneficiario del servicio, pues también puede corresponder, por ejemplo, a los anunciantes.

En el caso de los proveedores de acceso gratuito a Internet, de hecho quienes ofrecen una remuneración a los proveedores son quienes colocan anuncios o *pancartas* en páginas de Internet. Así pues, queda claro que estos servicios quedan cubiertos por la definición de servicios de comunicación electrónica y, por lo tanto, corresponden al ámbito de aplicación de la Directiva.

No obstante, sería aconsejable aclarar esta cuestión en el texto de la Directiva, pues no todos los lectores están al corriente de la interpretación que el Tribunal Europeo de Justicia ha dado de este término. Esto se podría hacer, por ejemplo, en el preámbulo de la Directiva.

III. Otras disposiciones jurídicas aplicables

Existen otros reglamentos comunitarios que tratan algunos aspectos relacionados con Internet. Cabe mencionar los siguientes instrumentos: la Directiva 1999/93/CE por la que se establece un marco comunitario para la *firma electrónica*[44], la Directiva 97/7/CE relativa a la protección de los consumidores en materia de contratos a distancia[45] y la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información (Directiva sobre el comercio electrónico)[46].

[42] Esta cuestión no se estudia en este documento.
[43] Asunto C-109/92 Wirth [1993] Rec I-6447, 15.
[44] Directiva 1999/93/CE de 13 de diciembre de 1999, por la que se establece un marco comunitario para la *firma electrónica*, Diario Oficial de las Comunidades Europeas, 19 de enero de 2000, L 13/12 a 13/20.
[45] Directiva 1997/7/CE de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a distancia, Diario Oficial de las Comunidades Europeas, 4 de junio de 1997, L 144.
[46] Directiva 2000/31/CE de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), Diario Oficial de las Comunidades Europeas, 17 de julio de 2000, L 178/1 a 178/16.

Sin embargo, la mayoría de estos reglamentos no establecen normas completas y específicas sobre protección de datos y en la mayor parte de los casos dejan la regulación de esta cuestión en manos de las Directivas específicas. Por ejemplo, en su considerando 14, la Directiva sobre el comercio electrónico dice que *"la protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva 95/46/CE y la Directiva 97/66/CE, que son enteramente aplicables a los servicios de la sociedad de la información (…) y, por tanto, no es necesario abordar este aspecto en la presente Directiva"*, y, en la letra b) del punto 5 del artículo 1, que *"la presente Directiva no se aplicará a cuestiones relacionadas con servicios de la sociedad de la información incluidas en las Directivas 95/46/CE y 97/66/CE"*.

El considerando 14 de la Directiva sobre comercio electrónico subraya que *"la aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso anónimo de redes abiertas como Internet"*.

No obstante, la Directiva sobre la *firma electrónica* establece, en su artículo 8, algunas normas específicas sobre protección de datos aplicables a los proveedores de servicios de certificación y a los organismos nacionales competentes en materia de acreditación o supervisión. Este artículo obliga a los Estados miembros a velar por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan los requisitos establecidos en la Directiva general sobre protección de datos. Además, esta disposición establece que los proveedores de servicios de certificación que expidan al público certificados únicamente puedan recabar datos personales directamente del titular de los datos o previo consentimiento explícito de éste, y sólo en la medida necesaria para la expedición y el mantenimiento del certificado. Los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento explícito de su titular.

De especial importancia es el apartado 3 del artículo 8 de esta Directiva, que estipula que, sin perjuicio de los efectos jurídicos concedidos a los seudónimos con arreglo al Derecho nacional, los Estados miembros no impedirán al proveedor de servicios de certificación que consigne en el certificado un seudónimo del firmante en lugar de su verdadero nombre.

El considerando 24 del preámbulo de esta Directiva destaca la importancia de que los proveedores de servicios de certificación observen la normativa sobre protección de datos y el respeto a la intimidad con objeto de aumentar la confianza del usuario en la comunicación y en el comercio electrónicos.

IV. Aplicación de las normativas nacionales sobre protección de datos y sus efectos internacionales

Las letras a) y b) del apartado 1 del artículo 4 de la Directiva regulan la aplicación de disposiciones nacionales de un Estado miembro cuando:

- "el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable;
- el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público".

La Directiva especifica que la noción de establecimiento implica el ejercicio efectivo y real de una actividad mediante una instalación estable, y que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto.

De acuerdo con lo establecido en la letra c) del apartado 1 del artículo 4 de la Directiva, los datos recogidos utilizando medios, automatizados o no, localizados en el territorio de la UE/EEE están sujetos a lo dispuesto en la normativa comunitaria sobre protección de datos.

El considerando 20 de esta Directiva amplía la explicación: "El hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; (considerando) que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva".

Aunque la interpretación de la noción de "equipos" o "medios" ha suscitado un debate sobre su alcance, determinados ejemplos quedan indudablemente dentro del ámbito de aplicación del artículo 4.

Éste será el caso, por ejemplo, de un fichero de texto instalado en el disco duro de un ordenador que recibirá, almacenará y devolverá información a un servidor ubicado en otro país. Dichos ficheros de texto, conocidos como *cookies*, se utilizan para recabar datos para un tercero. Si el ordenador se encuentra en un país de la UE y el tercero está fuera de la Comunidad, éste último aplicará los principios del Derecho nacional de ese Estado miembro a la recopilación de datos a través de la *cookie*.
En tal caso, de conformidad con el apartado 1 del artículo 4, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

V. Conclusiones

- En Internet se procesan grandes cantidades de datos personales a los que se aplican las Directivas sobre protección de datos.
- La Directiva general es aplicable en todos los casos, mientras que la Directiva específica lo es a los servicios de telecomunicación. Debido a la terminología utilizada en la Directiva 97/66/CE, a veces resulta difícil determinar si un servicio concreto se puede considerar de telecomunicación.
- La revisión del marco jurídico relativo a las telecomunicaciones ha ayudado a aclarar el ámbito de aplicación de la Directiva sobre intimidad y telecomunicaciones. Sin embargo, algunos aspectos pueden requerir aclaraciones adicionales, y especialmente la referencia a la necesidad de incluir la remuneración en la definición de servicios de comunicación electrónica. Para evitar posibles malentendidos en relación con el ámbito de aplicación de la Directiva, convendría recoger en su preámbulo la interpretación que el Tribunal Europeo de Justicia ha dado a este texto.
- La legislación europea sobre protección de datos debe aplicarse a los datos recabados con equipos, automatizados o no, situados en el territorio de la UE/EEE.

CAPÍTULO 4: CORREO ELECTRÓNICO

I. Introducción

No resulta fácil describir en pocas palabras la base técnica del correo electrónico, debido, principalmente, a los siguientes factores:

• Existen algunos *protocolos* oficiales pero, al igual que sucede con el *protocolo* HTTP, el grado de riesgo para la privacidad dependerá de cómo se ejecuten en la práctica. Existen miles de programas de servidores o clientes de correo electrónico diferentes y parece sumamente difícil sacar conclusiones generales, pues no se dispone de datos fiables sobre su utilización.

• Las operaciones invisibles de tratamiento que realizan esos programas son, como ya indica la palabra "invisible", difíciles de detectar. Además, los programas se están ampliando y complicando tanto que resulta casi imposible tener la certeza de que se han registrado todas las funciones, incluso las más ocultas.

En consecuencia, la descripción siguiente no puede considerarse exhaustiva y no siempre será representativa de lo que sucede diariamente en decenas de millones de ordenadores personales conectados a Internet en todo el mundo.

II. Agentes

Son varios los agentes que intervienen en el proceso de tratamiento de un mensaje de correo electrónico. Cada uno de ellos deberá tener en cuenta las cuestiones relativas a la protección de datos en cada fase del proceso. Estos agentes son[47]:

- El remitente del mensaje
- El destinatario del mensaje (titular de una dirección de correo electrónico)
- El proveedor del servicio de correo electrónico (servidor de correo que almacena el mensaje enviado a un usuario hasta que éste desea recibirlo)
- El proveedor de software que suministra al remitente el programa cliente de correo electrónico
- El proveedor de software que suministra al destinatario el programa cliente de correo electrónico
- El proveedor de software que suministra el programa servidor de correo.

III. Descripción técnica

Básicamente, un usuario que quiera utilizar el correo electrónico necesita:

• Un "programa cliente de correo electrónico", que es un programa instalado en el ordenador personal del usuario

• Una dirección de correo electrónico (una cuenta de correo electrónico)

[47] El operador de telecomunicaciones no participa específicamente en el proceso de envío de correo electrónico, pero desempeña un papel fundamental en la transmisión de señales que hace posible toda forma de comunicación por correo electrónico. Este agente tiene obligaciones específicas relativas a la seguridad establecidas por las Directivas.

- Una conexión a Internet.

Proceso de envío de un mensaje de correo electrónico

Existe una gran variedad de "programas clientes de correo electrónico", pero todos han de ceñirse a los estándares de Internet. El envío de un mensaje consta, básicamente, de los siguientes pasos:

- El usuario compone un mensaje en su "programa cliente de correo electrónico" y escribe en el campo del destinatario la dirección correspondiente.
- Al pulsar el botón "enviar" en el programa cliente de correo electrónico, un *proveedor de servicios de Internet* transferirá el mensaje al servidor de correo del destinatario, normalmente una organización, o al buzón de la cuenta de correo electrónico del usuario.
- Si el mensaje se envía al servidor de correo de una organización, éste lo transmitirá directamente al destinatario o, en su defecto, a un servidor de retransmisión ("retransmisión de salida").
- El mensaje puede pasar por distintos servidores de retransmisión hasta llegar al servidor de correo del destinatario.
- El destinatario estará directamente conectado al servidor de correo (por ejemplo, en una red de área local) o habrá de establecer una conexión para recibir el mensaje.

Direcciones de correo electrónico

Las direcciones de correo electrónico constan de dos partes separadas por el símbolo "@"; por ejemplo: john.smith@nowhere.com o subs34219@nowhere.org

- La parte derecha identifica el dominio en que el destinatario tiene la cuenta. Se trata en realidad de un nombre DNS referido a la dirección IP del servidor de correo.
- La parte izquierda describe la identificación única del destinatario. Es el nombre con el que el servidor de correo electrónico lo identifica. No existe ninguna obligación técnica de que sea el verdadero nombre del destinatario: puede consistir en un seudónimo escogido por el titular o un código arbitrario asignado por el servidor de correo en el proceso de registro.

Desde el punto de vista técnico, para enviar un mensaje de correo electrónico no es necesario identificarse. De hecho, sucede lo mismo que en el mundo real, donde una persona puede enviar una carta sin tener que dar su nombre. En el caso de la *buzonfia* ("spam"), en general el emisor no utilizará una cuenta de correo electrónico, sino que accederá directamente al *protocolo* SMTP, lo que le permitirá suprimir o modificar su dirección de correo electrónico.

***Protocolos* de correo electrónico**

Además del *protocolo* TCP/IP, en el correo electrónico se utilizan otros dos *protocolos*:

1. El primero es el *protocolo* simple de transferencia de correo (SMTP) y se utiliza para ENVIAR un correo de un cliente al servidor de correo del destinatario. El mensaje no se envía directamente al ordenador del destinatario, que puede no estar encendido o conectado a Internet cuando el emisor decida enviarlo. Esto significa que, para recibir un correo, el usuario de Internet debe disponer de un buzón de correo (una cuenta) en un

servidor. El proveedor de servicios de correo almacena el mensaje y espera a que el destinatario vaya a buscarlo.

2. El segundo es el *protocolo* POP y lo utiliza el destinatario para establecer una conexión con el servidor de correo y comprobar si tiene algún mensaje. Para ello, el destinatario tiene que introducir su nombre de buzón y su contraseña, de modo que nadie más pueda acceder a su correspondencia.

En general, los programas cliente de correo electrónico incluyen ambos *protocolos*, pues es probable que un usuario de Internet que quiera enviar un mensaje desee igualmente recibir una respuesta.

IV. Riesgos para la privacidad

Determinadas cuestiones conllevan riesgos específicos para la privacidad.

Recopilación de direcciones de correo electrónico

Como ya se ha mencionado, la dirección de correo electrónico es un elemento indispensable para establecer una conexión. Pero por otra parte, es también una valiosa fuente de información que contiene datos personales del usuario. Por lo tanto, es útil conocer los distintos métodos de recogida de direcciones de correo electrónico.

Existen distintas formas de recopilar direcciones de correo electrónico:

- El proveedor del "programa cliente de correo electrónico", que se compra o se obtiene de forma gratuita, solicita al usuario que se registre.
- También es posible introducir en los programas un código que transmitirá al proveedor de software la dirección de correo electrónico del cliente sin que éste se entere (tratamiento invisible).
- En algunos navegadores se han detectado fallos en la seguridad que permiten a un sitio web conocer las direcciones de correo electrónico de sus visitantes. Ello se puede hacer a través de contenidos activos malignos que utilicen, por ejemplo, un *JavaScript.*
- También es posible configurar algunos navegadores para que envíen la dirección de correo electrónico como una contraseña anónima cuando se establecen conexiones FTP (sin embargo, ésta no es una configuración por defecto).
- Algunos sitios web pueden solicitar la dirección de correo electrónico en distintas situaciones (por ejemplo, los sitios comerciales a la hora de realizar un pedido, un registro previo para acceder a una sala de charla, etc.).
- Hay otros modos de recabar direcciones de correo electrónico en espacios públicos en Internet[48].
- Existe la posibilidad de interceptar el correo electrónico durante la transmisión de un mensaje.

[48] La autoridad francesa en materia de protección de datos, conocida como CNIL, ha realizado otras investigaciones sobre la *buzonfia* y la recopilación de direcciones de correo electrónico. Véase, en particular, el informe de la CNIL sobre correo electrónico y protección de datos del 14 de octubre de 1999, disponible en el sitio web de la CNIL: www.cnil.fr.

Datos sobre tráfico

Resulta esencial establecer una distinción entre el contenido de un correo electrónico y los datos sobre tráfico, que son los datos que los *protocolos* necesitan para realizar correctamente la transmisión del emisor al destinatario.

Los datos sobre tráfico constan, por una parte, de la información que proporciona el emisor (por ejemplo, la dirección de correo electrónico del destinatario), y por otra de información técnica generada de forma automática durante el procesamiento del mensaje (como la fecha y la hora de envío o el tipo y la versión del "programa cliente de correo electrónico").

Todos los datos sobre tráfico o parte de ellos se colocan en una cabecera que se transmite al destinatario junto con el mensaje. El servidor de correo del receptor y el "cliente de correo" utilizan las partes transferidas de los datos sobre tráfico para tratar correctamente el mensaje entrante. El destinatario podría usar los datos sobre tráfico (propiedades del correo electrónico) con fines analíticos, como comprobar el camino seguido por el mensaje en Internet.

Se considera que los siguientes datos quedan incluidos en la definición de "datos sobre tráfico":

- dirección de correo electrónico y dirección IP del emisor
- tipo, versión e idioma del programa cliente
- dirección de correo electrónico del receptor
- fecha y hora de envío del correo electrónico
- tamaño del correo electrónico
- conjunto de caracteres utilizado
- tema del mensaje (esto ofrece también información sobre el contenido de la comunicación)
- nombre, tamaño y tipo de los documentos adjuntos
- lista de retransmisores SMTP utilizados.

En la práctica, normalmente los servidores de correo electrónico del emisor y del receptor almacenan los datos sobre tráfico. Esto también podrían hacerlo los servidores de retransmisión en el camino de comunicación a través de Internet.

Dado que la Directiva 97/66/CE no define formalmente los datos sobre tráfico, conviene señalar que algunos agentes de Internet podrían considerar erróneamente que los datos personales que no son necesarios para la comunicación ni para la facturación pero se generan durante la transmisión son datos sobre tráfico que pueden almacenar.

En su Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación[49], el Grupo de Trabajo del artículo 29 abordó algunos de los problemas de privacidad relacionados con datos sobre tráfico. El Grupo de Trabajo considera que los medios más eficaces para reducir riesgos inaceptables para la privacidad a la vez que se reconoce la necesidad de un cumplimiento efectivo de la legislación se basan en que los datos sobre tráfico no deberían, en principio, conservarse sólo con fines de cumplimiento de la ley, y en que las

[49] Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999, 5085/99/ES/final, WP 25.

normativas nacionales no deberían obligar a los operadores de telecomunicaciones, a los servicios de telecomunicaciones y a los *proveedores de servicios de Internet* a guardar los datos sobre tráfico durante un tiempo superior al necesario para efectuar la facturación.

En la declaración oficial de la Conferencia de autoridades europeas de protección de datos, celebrada en Estocolmo en la primavera de 2000, se señaló que en los casos específicos en que se han de conservar datos sobre tráfico deberá existir una necesidad demostrable, el período de conservación deberá ser lo más breve posible y la práctica deberá estar claramente regulada por la ley.

Contenido del correo electrónico

La confidencialidad de las comunicaciones está protegida por el artículo 5 de la Directiva 97/66/CE. En virtud del mismo, ninguna persona distinta de los usuarios podrá leer el contenido de un correo electrónico entre dos partes. Si durante la transmisión el contenido del mensaje se almacena en servidores de retransmisión, debería borrarse tan pronto como haya sido enviado.

Si un servidor de retransmisión no puede enviar un correo electrónico, podrá almacenarlo durante un período de tiempo breve y limitado hasta que se devuelva al emisor junto con un mensaje de error que le informe de que el correo electrónico no se pudo hacer llegar al destinatario.

El contenido de un correo electrónico se almacena en el servidor de correo hasta que el programa cliente de correo electrónico del usuario solicita su entrega. En algunos casos, el usuario puede optar por dejar el mensaje almacenado en el servidor de correo a pesar de tener una copia propia. Si el usuario no se decide por esta posibilidad, el servidor deberá borrar el mensaje lo antes posible una vez que tenga la certeza de que el destinatario lo ha recibido.

Si se realiza un control antivirus en forma de análisis de contenidos, éste deberá llevarse a cabo de forma automática y sólo con ese fin. Los datos no deberán analizarse con ningún otro propósito ni comunicarse a nadie, ni siquiera si se detecta algún virus.

Otro riesgo para la privacidad asociado al correo electrónico está relacionado con la incapacidad del usuario de eliminar de un modo fácil y eficaz un mensaje que ha enviado o recibido, pues la función de borrar no suprimirá necesariamente un correo del sistema. En ese caso puede resultar relativamente fácil para otro usuario del mismo ordenador o para un administrador del sistema, si se trata de un ordenador en red, recuperar un mensaje que el usuario original quería borrar y cree que ha desaparecido del sistema. Aunque el problema no es exclusivo del correo electrónico, resulta especialmente significativo en este contexto. Para solucionarlo, los sistemas deberían diseñarse de manera que la función de borrar eliminase realmente la información del sistema.

Para controlar el tráfico de una red se puede utilizar tanto el hardware como el software. Esto se conoce como *husmeo*. Los programas de *husmeo* pueden leer todos los paquetes de datos de una red y presentar en texto claro toda la comunicación no encriptada. La forma más sencilla de *husmeo* se puede realizar utilizando un ordenador personal normal conectado a una red, con programas que se pueden encontrar fácilmente.

Si el *husmeo* se realiza en nudos o empalmes centrales de Internet, esto permitiría interceptar y controlar a gran escala el contenido de mensajes de correo electrónico y los datos sobre tráfico de acuerdo con determinadas características, principalmente la presencia de palabras clave. Como actividad de control general y exploratoria, el *husmeo* sólo puede permitirse si se respetan las condiciones establecidas en el artículo 8 del

Convenio Europeo de Derechos Humanos, aun cuando lo lleven a cabo organismos gubernamentales.

En este contexto, resulta interesante señalar las preocupaciones actuales existentes en todo el mundo sobre un posible control de las comunicaciones internacionales y, en particular, sobre el sistema de interceptación de satélites "Echelon". La supervisión internacional es actualmente una cuestión candente en el programa de trabajo del Parlamento Europeo[50]. En un informe dirigido al Director General de Estudios del Parlamento Europeo[51] sobre el desarrollo de las tecnologías de supervisión y el riesgo de abuso de la información económica, se menciona que el sistema "Echelon" ha existido durante más de veinte años. De acuerdo con este informe, Echelon utiliza intensamente las redes mundiales de comunicación de la NSA[52] y el GCHQ[53] similares a Internet para permitir que centros remotos de información interroguen a ordenadores en cada sitio dedicado a la recopilación y reciban los resultados de forma automática.
Otro sistema de control polémico es Carnivore que, de acuerdo con la información publicada por el EPIC (Centro de Información sobre la Intimidad Electrónica)[54], controla el tráfico en las instalaciones de los *proveedores de servicios de Internet* con objeto de interceptar información de criminales sospechosos en el correo electrónico. El EPIC afirma que Carnivore podría analizar millones de mensajes de correo electrónico por segundo y permitir a los agentes encargados de velar por el cumplimiento de la ley interceptar todas las comunicaciones digitales de un cliente de un *proveedor de servicios de Internet*. El Congreso de Estados Unidos, los medios de comunicación y la comunidad de defensa de la privacidad han planteado preguntas muy serias sobre la legalidad de Carnivore y los abusos que puede conllevar su uso. En respuesta a las protestas públicas relacionadas con Carnivore, el 27 de julio de 2000 la Fiscal General Janet Reno anunció que se permitiría el acceso de un "grupo de expertos" a las especificaciones técnicas del sistema, con objeto de aliviar la preocupación pública.

El debate sobre la vigilancia mundial de las comunicaciones también forma parte del programa de trabajo del Consejo de Europa. El 27 de abril de 2000, el Comité de expertos en delitos del ciberespacio publicó su "proyecto de Convenio sobre delincuencia en el ciberespacio"[55]. Este Convenio obligaría a las empresas que ofrecen servicios de Internet a recoger y almacenar datos destinados a los organismos públicos encargados de velar por el cumplimiento de la ley, con lo que facilitaría la recopilación de información. Sería necesario un intercambio de tales datos entre autoridades gubernamentales de distintos países, incluso los que no son parte en el Convenio Europeo de Derechos Humanos u otros instrumentos del Consejo de Europa o de la UE en materia de protección de datos. Hasta la fecha, no se ha previsto ningún requisito sustancial para proteger el derecho fundamental a la intimidad y la protección de los datos personales en terceros países que reciben datos de carácter personal sobre ciudadanos de la UE, y tampoco se han establecido los principios básicos para respetar las normas relativas a derechos humanos fundamentales como la necesidad y la proporcionalidad.
Aunque su intención no es comentar el texto del proyecto de Convenio, el Grupo de Trabajo desearía recordar el punto de vista presentado por las autoridades europeas de

[50] Para más información, consúltese la Comisión de Libertades y Derechos de los Ciudadanos, Justicia y Asuntos Interiores del Parlamento Europeo: http://www.europarl.eu.int/committees/es/default.htm. Véase también EPIC, Alert 7.07, 20 de abril de 2000.
[51] Informe sobre las capacidades de interceptación en 2000, mayo de 1999.
[52] Agencia nacional de seguridad, Estados Unidos.
[53] Centro gubernamental de comunicaciones, homólogo británico de la NSA.
[54] EPIC Alert 7.15, 3 de agosto de 2000.
[55] El texto del proyecto se encuentra a disposición del público en: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

protección de datos en una declaración realizada en abril de 2000 durante la Conferencia de Estocolmo, en la que señalaron con preocupación que, según las propuestas presentadas, los *proveedores de servicios de Internet* deberían almacenar habitualmente los datos sobre tráfico no sólo con fines de facturación, con objeto de permitir un posible acceso de los organismos encargados de velar por el cumplimiento de la ley.
La Conferencia señaló que esta retención constituiría una invasión ilegal de los derechos fundamentales que garantiza el artículo 8 del Convenio Europeo de Derechos Humanos y declaró que en los casos específicos en que se hayan de conservar datos sobre tráfico, debería existir una necesidad demostrable, el período de conservación debería ser lo más breve posible y la práctica debería estar claramente regulada por la ley.

En su Recomendación 2/99[56], el Grupo de Trabajo del artículo 29 ha tratado los aspectos que afectan a la privacidad en la interceptación de las comunicaciones. En esta Recomendación, el Grupo de Trabajo señala que cualquier interceptación de las telecomunicaciones, definida como el conocimiento por un tercero de los datos sobre el contenido y el tráfico de las telecomunicaciones privadas entre dos o más corresponsales y, en especial, de los datos sobre tráfico relacionados con la utilización de servicios de telecomunicación, constituye una violación del derecho individual a la privacidad y a la confidencialidad de la correspondencia. De esto se desprende que las interceptaciones son inaceptables, a menos que cumplan tres criterios fundamentales, de conformidad con lo dispuesto en el apartado 2 del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales del 4 de noviembre de 1950[57] y de la interpretación que el Tribunal Europeo de Derechos Humanos ha hecho de esta disposición: un fundamento jurídico, la necesidad de la medida en una sociedad democrática y la conformidad con alguno de los objetivos legítimos enumerados del Convenio[58].

V. Análisis de cuestiones especiales

Correo web

Los sistemas de correo electrónico que utilizan páginas web como interfaz se conocen como "*correo web*" (por ejemplo, Yahoo, Hotmail, etc.). Se puede acceder al *correo web* desde cualquier lugar y el usuario no necesita conectarse a un determinado *proveedor de servicios de Internet*, como cuando utiliza una cuenta normal de correo electrónico.

El *correo web* suele ser gratuito, pero para obtener su cuenta a menudo los usuarios se ven obligados a comunicar al proveedor datos personales. De acuerdo con las investigaciones realizadas por las autoridades responsables de la protección de datos, parece ser que muchos proveedores de *correo web* venden o comparten datos de carácter personal con fines comerciales.

El *correo web* utiliza el *protocolo* HTML, en lugar del POP, para leer y controlar el correo electrónico. De hecho, los mensajes se muestran en una página HTML clásica.

[56] Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18.
[57] Conviene destacar que las garantías fundamentales reconocidas por el Consejo de Europa en relación con la interceptación de telecomunicaciones establecen obligaciones para los Estados miembros independientemente de las distinciones hechas en la Unión Europea de acuerdo con la naturaleza comunitaria o intergubernamental de los campos abordados.
[58] El Convenio nº 108 del Consejo de Europa estipula igualmente que la interceptación sólo puede permitirse cuando en una sociedad democrática resulta necesaria para la protección de los intereses nacionales enumerados en el apartado segundo del artículo 9 de dicho Convenio y está estrictamente definida en función de esta finalidad.

Esta característica permite al proveedor de servicios de correo incorporar anuncios personalizados en la página HTML en la que éste se presenta (gráficamente, fuera del propio mensaje). El *correo web* depende en gran medida de patrocinadores y visualiza gran cantidad de *pancartas* publicitarias.

Dado que los sistemas de *correo web* se basan en el *protocolo* HTTP, pueden ser vulnerables a los "Web bugs", que permiten descubrir la identidad de correo electrónico de una persona mediante *cookies* y etiquetas HTML incrustadas.

Los proveedores de *correo web* no deben incorporar *hipervínculos* invisibles en páginas web en las que la cuenta de correo electrónico forma parte del URL. Si lo hacen, ayudan a transmitir la dirección de correo electrónico del titular de los datos a la empresa de publicidad. Ésta es otra forma de invasión de la privacidad del usuario con un tratamiento invisible.

Guías

Existen distintos servicios en Internet que ofrecen guías de direcciones de correo electrónico. Estas guías públicas están sujetas a las mismas normas que las telefónicas y otros datos a disposición del público, como se explicará en el capítulo 6. En el marco jurídico vigente, el usuario debe disponer al menos del derecho a oponerse al tratamiento de sus datos, de acuerdo con el artículo 14 de la Directiva 95/46/CE y con el artículo 11 de la Directiva 97/66/CE.

Cabe señalar que el borrador de la directiva revisada sobre el tratamiento de datos de carácter personal y la protección de la privacidad en el sector de las telecomunicaciones armoniza las obligaciones de los responsables de los datos a este respecto y ofrece a los titulares de dichos datos el derecho de aprobar su incorporación en guías. El Grupo de Trabajo considera que éste es un avance importante.

Buzonfia

La *buzonfia* se puede definir como el envío de correos electrónicos no solicitados, de naturaleza generalmente comercial, en grandes cantidades y de forma repetida a personas con las que el emisor no ha tenido ningún contacto previo[59]. El Grupo de Trabajo del artículo 29 ya abordó esta cuestión en su Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico[60].

Desde el punto de vista de los ciudadanos, el problema presenta tres aspectos: en primer lugar, la recopilación de la dirección de correo electrónico de una persona sin su consentimiento o conocimiento; en segundo lugar, la recepción de grandes cantidades de publicidad no deseada, y por último, el coste del tiempo de conexión.

Las direcciones de correo electrónico pueden recabarse en guías públicas o empleando distintas técnicas. Por ejemplo, el propio usuario puede dar su dirección de correo electrónico al comprar bienes o servicios en Internet. En otros casos, un proveedor puede vender a terceros la dirección que el usuario le ha proporcionado.

De acuerdo con el Grupo de Trabajo, las normas de la Directiva sobre protección de datos ofrecen una respuesta clara a las cuestiones sobre privacidad que plantea la *buzonfia* y establecen una imagen nítida de los derechos y obligaciones de los participantes. Conviene distinguir dos situaciones:

[59] Véase el informe de la CNIL sobre correo electrónico y protección de datos, 14 de octubre de 1999.
[60] Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, presentado por el Grupo operativo sobre Internet, aprobado el 3 de febrero de 2000, 5007/00/ES/final, WP 28.

- Si una empresa obtiene una dirección de correo electrónico directamente de una persona con vistas a realizar un envío de correo electrónico comercial o a que lo realice un tercero al que ha revelado los datos, la empresa original debe informar a la persona de esos propósitos al recopilar la dirección[61]. Además, desde el momento en que comunica su dirección, el titular de los datos debe contar con el derecho mínimo de oponerse al uso de sus datos con medios electrónicos sencillos, como marcar una casilla prevista para este fin por la empresa original, en primer lugar, y por las empresas que han recibido datos de la empresa original, posteriormente[62]. Determinadas legislaciones nacionales de aplicación de las directivas pertinentes incluso obligan a la empresa a solicitar el consentimiento del titular de los datos. Los requisitos recogidos en el artículo de la Directiva sobre comercio electrónico referentes a las comunicaciones comerciales no solicitadas completan estas normas a escala técnica imponiendo la obligación de consultar un registro sobre el proveedor de servicios, sin perjuicio alguno de las obligaciones generales aplicables a los responsables de los datos.
- Si una dirección de correo electrónico se recaba en un espacio público en Internet, su uso para envío de correo electrónico comercial no solicitado podría incumplir la legislación comunitaria pertinente por tres motivos: en primer lugar, podría considerarse un tratamiento desleal de datos de carácter personal en virtud de la letra (a) del apartado 1 del artículo 6 de la Directiva general; en segundo lugar, iría en contra del "principio de finalidad" recogido en la letra (b) del apartado 1 del artículo 6 de dicha Directiva, pues el titular de los datos publicó su dirección de correo electrónico para un fin diferente, como la participación en un foro de debate; por último, teniendo en cuenta el desequilibrio de costes y las molestias que sufre el destinatario, el envío de dichos mensajes no podría considerarse satisfactorio de acuerdo con el equilibrio de intereses estipulado en la letra (f) del artículo 7[63].

Una característica específica del envío de mensajes comerciales de correo electrónico es que, mientras que el coste para el emisor es muy reducido comparado con los métodos tradicionales de venta directa, implica un gasto para el receptor en términos de tiempo de conexión. Esta situación constituye un claro incentivo para utilizar esta herramienta de comercialización a gran escala sin prestar atención a las cuestiones relativas a la protección de datos y los problemas provocados por el correo electrónico comercial.

El coste del correo electrónico no solicitado recae tanto en el receptor como en el proveedor de correo Internet del receptor, que puede ser el servidor de *correo web* o el *proveedor de servicios de Internet* del destinatario.

El servidor de correo tiene que almacenar durante cierto tiempo los mensajes de correo electrónico no solicitados. Por su parte, el receptor ha de pagar[64] para descargar un mensaje que no desea leer y pierde tiempo clasificando los mensajes recibidos y eliminando los no solicitados, sobre todo cuando los mensajes de *buzonfia* no aparecen identificados como tales en la casilla destinada al tema, lo que se suele hacer mediante un

[61] Artículo 10 de la Directiva 95/46/CE.

[62] Artículo 14 de la Directiva 95/46/CE.

[63] En él se requiere (uno de los posibles fundamentos legítimos del tratamiento) que el tratamiento de datos sea "necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento… siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado".

[64] El operador de telecomunicaciones cuando el abonado utiliza un *módem.* En otro caso, si el usuario emplea una línea arrendada, aunque el coste no aumente inmediatamente a causa del mensaje de *spam* (tarifa plana), desde un punto de vista macroeconómico resulta evidente que los costes indirectos del tráfico relacionados con la *buzonfia* masiva se cargan al *proveedor de servicios de Internet*, con las consecuencias que esto conlleva para los precios de las líneas arrendadas.

código "ADV:" de anuncio en los primeros caracteres de dicha casilla. Se estima que la *buzonfia,* también conocida como correo basura, constituye actualmente el diez por ciento del total del correo electrónico mundial[65].

VI. Aspectos de seguridad y confidencialidad

El correo electrónico ofrece las mismas posibilidades de comunicación que el tradicional, por lo que se le aplican las mismas normas que a la inviolabilidad de la correspondencia.

Todo el mundo tiene derecho a enviar un mensaje por correo electrónico a otra persona sin que un tercero lo lea. El artículo 5 de la Directiva 97/66/CE, que cubre las comunicaciones y los correspondientes datos sobre tráfico enviados, por ejemplo, por correo electrónico, establece las obligaciones aplicables a la confidencialidad de las comunicaciones. Junto con estas obligaciones, el artículo 4 de esa misma Directiva obliga a los proveedores de servicios públicos de telecomunicación a adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y a informar a los usuarios sobre un riesgo concreto de violación de la seguridad y sobre las posibles soluciones, incluidos los costes necesarios.

En el mundo no electrónico, cualquier persona puede enviar cartas anónimas o firmadas con un seudónimo. Para poder enviar un mensaje anónimo de correo electrónico, varios proveedores de este servicio ofrecen al abonado la posibilidad de obtener direcciones anónimas de correo electrónico.

Desde el punto de vista del usuario, son varias las cuestiones pertinentes según el tipo de correo electrónico:

- La confidencialidad, que es la protección de los datos transmitidos contra la curiosidad de terceros. Una posible forma de garantizar la confidencialidad consiste en *encriptar* el mensaje que se va a enviar.

La *encriptación* y la desencriptación se basan en software complementario de los programas habituales de correo electrónico (programas accesorios) o en programas de correo electrónico y navegadores que ofrecen estos servicios. La resistencia de la *encriptación* depende de los algoritmos y la longitud de las claves utilizadas.

- La *integridad,* que es una garantía de que la información no sufrirá alteraciones de forma accidental o intencionada. La *integridad* puede obtenerse calculando un código especial basado en el texto que se transferirá encriptado junto con el propio texto. El receptor podrá entonces descifrar el código y, volviéndolo a calcular, comprobar si el mensaje ha sido modificado.

- La *autentificación,* que garantiza que un usuario es realmente quien afirma ser. La *autentificación* se puede verificar mediante el intercambio de *firmas digitales* basadas en *certificados electrónicos*. No es necesario que dichos certificados mencionen el verdadero nombre del abonado, que, en virtud de lo establecido en el artículo 8 de la Directiva relativa a la *firma electrónica*[66], puede sustituirse por un seudónimo.

[65] Véase la página 3 del libro *Net Worth (op. cit.)*.

[66] Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la *firma electrónica*, Diario Oficial de las Comunidades Europeas, 19 de enero de 2000, L 13/12 a 13/20.

VII. Medidas en favor de la privacidad[67]

Dos tipos de herramientas merecen una mención especial en este capítulo: los filtros de correo electrónico y el correo electrónico anónimo[68].

1) Los filtros de correo electrónico analizan todo el correo electrónico entrante de un usuario y sólo dejan pasar los mensajes que éste ha indicado que desearía recibir. Está muy extendido el uso de estos sistemas para eliminar la *buzonfia*.
Actualmente varias empresas ofrecen herramientas que los usuarios de Internet pueden instalar en sus ordenadores para descartar el correo electrónico no deseado. Además, varios paquetes de correo electrónico permiten a los abonados filtrar los mensajes conforme aparecen en el escritorio.
Los filtros más eficaces son los que permiten la entrada exclusiva de determinados mensajes de correo electrónico. Sin embargo, aunque este sistema es útil para las personas que disponen de una red permanente de corresponsales de correo electrónico, resultaría incómodo para la mayoría de la población, pues requeriría la aprobación de cada nuevo corresponsal.
Las tecnologías de filtrado más habituales permiten la entrada de todos los mensajes excepto los que proceden de determinados nombres de dominio o direcciones o los que contienen determinadas palabras clave en la línea destinada al tema. Sin embargo, los emisores pertinaces modifican a menudo su nombre de dominio o su dirección para poder atravesar los filtros, pues normalmente las cuentas de correo electrónico basadas en la Web son gratuitas y resulta sencillo incorporarse a ellas o dejarlas en cualquier momento. Por último, debido a las elevadas posibilidades de error, resulta difícil realizar un filtrado eficaz utilizando palabras clave.

2) El correo electrónico anónimo permite a los usuarios comunicar en línea su dirección de correo electrónico sin tener que revelar su identidad[69]. Actualmente se puede disponer de este servicio de forma gratuita en Internet gracias a varias empresas que realizan servicios de "reenvío".

Con estos servicios, el responsable del reenvío elimina la identidad del usuario de los mensajes que éste ha enviado. Las respuestas al correo electrónico anónimo van al responsable del reenvío, quien vincula la dirección anónima a la verdadera y entrega la respuesta al cliente de un modo seguro.

VIII. Conclusiones

Desde el punto de vista de la protección de datos, se deben abordar las siguientes cuestiones relacionadas con el correo electrónico:

Tratamiento invisible realizado por "clientes de correo" y retransmisores SMTP

El titular de los datos debería disponer de la oportunidad de permanecer en el anonimato en la mayor medida posible, sobre todo cuando participa en un foro de debate. Parece ser que junto con el contenido del mensaje a menudo se envían las direcciones de correo electrónico de los participantes en estos foros[70]. Esto contraviene el artículo 6 de la

[67] Para más detalles, véase el capítulo 9, sobre medidas en favor de la privacidad.
[68] Véanse las páginas 275 y siguientes del libro *Net Worth (op. cit.)*,.
[69] Este documento se refiere también a este tipo de servicio en el apartado V del capítulo 6 (publicaciones y foros), relativo a las medidas sobre protección de la intimidad.
[70] Para más detalles, véase el capítulo 6.

Directiva 95/46/CE, que limita el tratamiento de la información a los casos en que sea necesario con fines legítimos[71].

Conservación de datos sobre tráfico por intermediarios y proveedores de servicios de correo

En virtud del artículo 6 de la Directiva 97/66/CE, los datos sobre tráfico deberán destruirse en cuanto termine la comunicación. La Directiva sólo establece determinadas excepciones a este principio, por ejemplo, cuando es necesario realizar un tratamiento mayor para efectuar la facturación[72].

Interceptación

La interceptación del correo electrónico (la comunicación y los correspondientes datos sobre tráfico) es ilegal, a menos que así se haya dispuesto por ley en circunstancias concretas de acuerdo con el Convenio Europeo de Derechos Humanos y la Directiva 97/66/CE. En cualquier caso, debe prohibirse el *husmeo* a gran escala. El principio de especificidad, corolario de la prohibición de toda vigilancia general o exploratoria, implica que, en lo que respecta a los datos sobre tráfico, las autoridades públicas sólo pueden acceder a los datos sobre tráfico de forma individual y nunca de forma proactiva ni como norma general[73].

Almacenamiento y análisis del contenido del correo electrónico

El contenido del correo electrónico debe mantenerse en secreto y se ha de impedir que los intermediarios y proveedores de servicios de correo puedan leerlo, incluso con "fines de seguridad en la red". Si se utiliza un programa antivirus para analizar documentos adjuntos, éste debe ofrecer suficientes garantías de confidencialidad. Si se detecta algún virus, el proveedor de servicios deberá tener la capacidad necesaria para avisar al emisor, pero ni siquiera en este caso deberá leer el contenido del mensaje ni de los documentos adjuntos.

El Grupo de Trabajo del artículo 29 recomienda encarecidamente la *encriptación* del contenido del correo electrónico, sobre todo cuando contiene información delicada de carácter personal. Los proveedores de servicios de correo electrónico deberían poner a disposición del público herramientas gratuitas de fácil utilización para encriptar el contenido de los mensajes. Además, los proveedores deberían ofrecer al abonado la oportunidad de descargar el correo desde el servidor del proveedor al ordenador cliente del usuario con una conexión segura. Debería tenerse igualmente en cuenta la necesidad de *integridad* y *autentificación*.

Correo electrónico no solicitado (*buzonfia*)

Si una empresa obtiene una dirección de correo electrónico directamente de una persona con vistas a realizar un envío de correo electrónico comercial no solicitado o a que lo

[71] Este principio se desarrolla en mayor medida en la Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, adoptada por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17.

[72] Véase también la Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada por el Grupo de Trabajo el 7 de septiembre de 1999.

[73] Véase, en este contexto, la Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18.

realice un tercero al que ha revelado los datos, la empresa original debe informar a la persona de esos propósitos al recopilar la dirección. Además, desde el momento en que comunica su dirección el titular de los datos debe contar con el derecho mínimo de oponerse al uso de éstos con medios electrónicos sencillos, como marcar una casilla prevista para este fin por la empresa original, en primer lugar, y por las empresas que han recibido datos de la empresa original, posteriormente

Si una dirección de correo electrónico se recaba en un espacio público en Internet, su uso para envío de correo electrónico comercial no solicitado podría incumplir la legislación comunitaria pertinente.

Guías de correo electrónico

Al igual que sucede con las guías telefónicas, el titular de los datos debe tener la posibilidad de decidir su exclusión de las mismas en virtud de los principios anteriormente mencionados de limitación de finalidad (letra b del apartado 1 del artículo 6 de la Directiva 95/46/CE) y del derecho a solicitar que no se le incluya en una guía (artículo 11 de la Directiva 97/66/CE). Además, se debería ofrecer al titular de los datos la posibilidad de aparecer en una guía especial de direcciones de correo electrónico que no se pueda utilizar con fines de venta directa.

Es importante tener en cuenta que en la versión actual de la propuesta de Directiva relativa a la protección de la intimidad en el sector de las telecomunicaciones este derecho de exclusión se transformará en un derecho de consentimiento, lo que constituye un avance importante a favor de los titulares de los datos.

CAPÍTULO 5: NAVEGACIÓN Y BÚSQUEDA

I. Introducción

Tal vez la actividad más habitual de los usuarios de Internet consiste en visitar páginas web con el fin de obtener información, lo que conlleva la visualización pasiva de su contenido. También es posible interactuar con los sitios web de un modo más activo. A menudo, el usuario de Internet ha de pulsar en un *hipervínculo*, entrar en un anuncio de la pantalla (*pancarta*) o completar un formulario con más información. El conjunto de estas actividades se denominará "navegación por la Web". En la práctica, esto se realiza mediante un navegador que conecta al usuario de Internet con un servidor web en alguna parte de Internet.

Desde el punto de vista de la protección de datos, cabe plantear tres cuestiones:

- ¿Qué información se genera sobre las actividades del usuario de Internet mientras éste navega por la Web?
- ¿Dónde se almacena esta información?
- ¿Qué información es necesaria para la prestación de los servicios que ofrecen los sitios web?

La última cuestión, que se refiere a los datos personales que un usuario de Internet comunica de forma voluntaria y a las condiciones en que los revela, no se tratará aquí, pues este capítulo se centra en las informaciones personales inherentes al proceso (técnico) de navegar por Internet y ofrece un esquema de las etapas posteriores en el proceso de navegación, así como una indicación de los datos de carácter personal que se generan.

II. Descripción técnica y agentes participantes

El proceso de navegación por la Web

• Proveedores de telecomunicaciones. Para contactar con un sitio web, normalmente un usuario de Internet entra en la Red a través de una conexión telefónica con un *proveedor de servicios de Internet*. El proveedor de telecomunicaciones registra la llamada al *proveedor de servicios de Internet*.

• Proveedor de acceso a Internet. El punto de entrada al *proveedor de servicios de Internet* es el servidor de acceso a la red. Por lo general, este servidor registra la *identificación de la línea de llamada* que solicita la conexión. La mayoría de los proveedores de acceso a Internet registran también el nombre de conexión, la hora de conexión y desconexión y la cantidad de datos transferidos en el transcurso de la sesión. Conviene señalar que, en algunos casos, el proveedor de acceso a Internet es también el proveedor de telecomunicaciones.

• Asignación de la dirección IP. Una vez establecido contacto con el proveedor de acceso a Internet, éste asigna una dirección IP dinámica para la sesión del usuario de Internet[74]. Desde entonces, todas las comunicaciones de la sesión se realizan desde y hacia esa dirección IP. El número IP acompaña a todos los paquetes transmitidos en las etapas siguientes de comunicación. El número IP asignado pertenece siempre a un conjunto

[74] A veces, un mismo usuario utiliza direcciones IP estáticas durante un largo período de tiempo. Este tipo de direcciones IP se suelen emplear cuando se utilizan tecnologías alternativas de acceso (líneas *ADSL*, televisión por cable, telefonía móvil). Al generalizarse estas tecnologías se está observando un aumento relativo de la utilización de direcciones IP estáticas.

determinado de números asignado al proveedor de acceso a Internet. Así, terceras partes externas pueden identificar fácilmente al *proveedor de servicios de Internet* del que provienen los paquetes IP[75, 76].

Posteriormente, el tráfico de Internet se clasifica en el *proveedor de servicios de Internet* por el número de puerto, que especifica el servicio y el *protocolo* correspondiente. En general, las solicitudes para visitar un sitio web se realizan mediante el *protocolo* HTTP. En el *proveedor de servicios de Internet*, este tráfico se reconoce por un número de puerto determinado. También puede transferirse directamente a un *encaminador* que conecta al usuario de la Red con los sitios web externos solicitados.

A menudo, la solicitud se transmite a un *servidor proxy* dedicado que registra la solicitud de un determinado sitio web. El *servidor proxy* guarda una copia del contenido de los sitios web más visitados. Si el sitio solicitado por el usuario de Internet se encuentra en el *servidor proxy*, éste sólo tiene que pedir al sitio correspondiente una actualización con los cambios que se hayan producido desde el momento en que se almacenó la copia. Esta medida reduce enormemente la cantidad de datos que han de intercambiar el *proveedor de servicios de Internet* y el sitio web, porque basta con que se comuniquen cambios y no páginas completas. El *servidor proxy* puede mantener una lista pormenorizada de visitas a sitios web conectados a una dirección IP en un momento determinado. Éstas pueden relacionarse con un usuario en particular mediante la dirección IP y el registro de las horas de la sesión.

• *Encaminadores*. En su camino entre el *proveedor de servicios de Internet* y el sitio web visitado, por lo general el tráfico pasa por varios *encaminadores* que dirigen los datos entre la dirección IP del usuario de Internet y la dirección IP del sitio web. Respecto al almacenamiento de datos de carácter personal, estos *encaminadores* se consideran elementos neutrales, aunque se puedan aplicar en ellos recursos dedicados destinados a interceptar el tráfico de Internet.

• Sitios web muy visitados. Una vez establecida la conexión con el sitio web, éste recaba información sobre el usuario de Internet que lo visita. Todas las solicitudes van acompañadas de la dirección IP de destino. El sitio web sabe igualmente desde qué página ha llegado el usuario, es decir, conoce la referencia de la página previa o URL. La información sobre las visitas al sitio web se almacena habitualmente en el "fichero histórico común". Todos los datos mencionados anteriormente pueden utilizarse con el fin de acumular, mediante un analizador de registros, información sobre el tráfico procedente de un sitio web o con destino a éste, así como sobre las actividades de los visitantes.

Tras conectar con un sitio web, en la comunicación entre los programas de navegación más utilizados por los usuarios de Internet y los sitios web visitados se recoge información adicional. Esto se conoce como "datos de charloteo", que suelen constar de los siguientes elementos[77]:

- Sistema operativo
- Tipo y versión del navegador
- *Protocolos* utilizados en la navegación
- Página remitente
- Preferencias de idioma

[75] En algunos casos, también otras partes, tales como universidades, organizaciones o empresas, pueden desempeñar el papel de *proveedores de servicios de Internet*.
[76] Hasta cierto punto, las direcciones IP también se asignan con criterios geográficos.
[77] Para más detalles, véase el capítulo 2.

- *Cookies*

La instalación de *cookies*[78] permite al sitio web disponer de mayor capacidad de recogida de información. Se trata de datos que pueden almacenarse en ficheros de texto en el disco duro del usuario y de los que el sitio web puede conservar una copia. Forman parte del tráfico HTTP, por lo que se pueden transportar sin problemas con el tráfico IP. Una *cookie* puede contener un número único (identificador global único) que permite realizar una mejor identificación que las direcciones IP dinámicas. Estas *cookies* aumentan la capacidad de los sitios web de almacenar y "personalizar" la información sobre sus visitantes. El sitio puede releer la *cookie* de forma periódica con objeto de identificar a un usuario de Internet y reconocerlo cuando vuelva a visitar el sitio, comprobar posibles contraseñas, analizar el camino que ha seguido durante una sesión y dentro de un sitio, registrar transacciones (por ejemplo, adquisición de artículos), personalizar un sitio, etc.

Existen *cookies* de distinta naturaleza: las hay permanentes y de duración limitada, en cuyo caso se llaman "*cookies* de sesión". Algunas pueden resultar útiles para ofrecer un determinado servicio en Internet o para simplificar la navegación. Por ejemplo, algunos sitios web utilizan *cookies* para identificar a sus usuarios cada vez que éstos los vuelven a visitar, de modo que no es necesario que se registren cada vez que quieren consultar las novedades.

Sin embargo, no se deben subestimar las consecuencias del uso de *cookies* en la privacidad. Esta cuestión se abordará en el apartado de este capítulo dedicado al análisis jurídico.

- *Portales*

Debido a la complejidad creciente de Internet, sus usuarios se conectan a menudo a un sitio web a través de los llamados *portales*, que ofrecen una presentación ordenada de vínculos web.

Los *portales* suelen contener vínculos con sitios comerciales y podrían compararse con un centro comercial electrónico que aloje gran cantidad de tiendas. Recopilan información de la misma forma que cualquier sitio web, pero también pueden almacenar información sobre las visitas a todos los sitios existentes "tras" el *portal*.

Los *portales* siempre están alojados por un *proveedor de servicios de Internet*, que en ocasiones puede incluso ser su propietario. En estos casos, el *proveedor de servicios de Internet* tiene la posibilidad de recabar datos sobre las visitas de un usuario a los sitios que se encuentran "tras" su *portal* y puede, por tanto, elaborar un perfil completo del usuario.

En un informe[79] sobre Internet y la privacidad basado en investigaciones realizadas sobre 60 *proveedores de servicios de Internet* de los Países Bajos, la autoridad holandesa en materia de protección de datos (*Registratiekamer*) llegó a la conclusión de que el proveedor de contenidos (en este caso, el *proveedor de servicios de Internet* propietario del *portal*) puede llegar a saber cuántos anuncios se han colocado, con qué frecuencia ha visitado el usuario una tienda electrónica, qué productos ha comprado y cuánto ha pagado por ellos.

- *Proveedores de servicios adicionales*

[78] En este caso nos referimos a las *cookies* permanentes, es decir, a las que permanecen más de una sesión.

[79] Véase el informe de la Registratiekamer (ARTZ, M.J.T. y VAN EIJK, M.M.M.), *Klant in het web: Privacywaarborgen voor Internettoegang*, Achtergrondstudies en verkenningen, 17 de junio de 2000, disponible en: www.registratiekamer.nl. Este informe subraya que casi todos los proveedores de acceso a Internet de los Países Bajos poseen su propia página de inicio, que también se utiliza como *portal* para iniciar la navegación.

En ocasiones, los datos recabados por los sitios web se transmiten (automáticamente) a un tercero que no forma parte de la comunicación original (por ejemplo, empresas especializadas en el análisis estadístico de la Web, como Nedstat). La finalidad de esta práctica puede ser almacenar datos estadísticos sobre las visitas al sitio web para venderlos posteriormente a los propietarios de dichos sitios. A menudo, las *pancartas* publicitarias recopilan mediante *cookies* información sobre los sitios web que una persona ha visitado. Algunos proveedores de servicios, como DoubleClick o Globaltrash, almacenan la información relativa a las visitas a los sitios web en los que han colocado anuncios. Con estos datos se puede elaborar un perfil de las preferencias de los usuarios de Internet que se utilizará posteriormente para personalizar páginas web.

La navegación desde el punto de vista del usuario de Internet

En muchos casos, un ordenador personal en el que se haya instalado un programa de navegación cargará automáticamente, una vez encendido, una página de inicio seleccionada en la Web. Esta página puede contener *hipervínculos* que pueden activarse para visitar otros sitios web o motores de búsqueda. Mientras navega, el programa de navegación del usuario de Internet envía una petición a un servidor situado en cualquier parte del mundo para que transmita una página web específica, identificada con su URL, alojada en dicho servidor web. Al hacer clic en un *hipervínculo*, en realidad el usuario de Internet está descargando en su ordenador la página web solicitada.

Tras conectarse a su *proveedor de servicios de Internet*, el usuario de Internet escoge uno de los siguientes métodos de navegación:

- Desplazarse directamente al sitio web solicitado introduciendo su URL; por ejemplo, www.amazon.com. El URL también contiene el *protocolo*.
- Llegar al sitio web mediante un sitio remitente (*portal)* que contiene *hipervínculos* a otros sitios. Estos *portales* están adquiriendo mayor popularidad a medida que aumenta el número de páginas web existentes y los usuarios de Internet necesitan orientación para encontrar la información que les interesa.
- Encontrar sitios interesantes introduciendo primero consultas en motores de búsqueda, que recurren a la indización por medio de palabras clave. El usuario introduce una o varias palabras clave e inicia la búsqueda. El motor de búsqueda comienza entonces a buscar los títulos de los sitios correspondientes y sus direcciones URL en su base de datos de índices. Puede reunir perfiles personales a medida que acumula los términos de búsqueda introducidos por un usuario de Internet y los sitios web visitados posteriormente. La personalización se realiza a menudo por medio de *cookies*. Algunos motores de búsqueda ofrecen también servicios más personalizados para los cuales se pide al usuario de Internet que proporcione información sobre sus preferencias personales con el fin de obtener, por ejemplo, actualizaciones periódicas de sitios web sobre un tema determinado[80].

Visión de conjunto de los datos más importantes que se generan y almacenan en las distintas fases del proceso de navegación por la Web

	Datos generados y/o almacenados	Observaciones
1. Proveedor de	Datos sobre tráfico de la conexión con	Puede ser el mismo que el

[80] En este contexto cabe mencionar la posición común sobre los motores de búsqueda adoptada por el Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones en la reunión celebrada en Hong Kong el 15 de abril de 1998, disponible en: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm.

telecomunicaciones	el *proveedor de servicios de Internet*	*proveedor de servicios de Internet*
2. *Proveedor de servicios de Internet*: servidor de acceso a la Red	*Identificación de la línea de llamada,* dirección IP, datos de sesión	
3. *Proveedor de servicios de Internet: proxy*	Páginas web visitadas por la dirección IP en un momento determinado	
4. *Encaminadores*	Dirección IP	
5. Sitios web	Dirección IP URL de la página anterior Datos de sesión (hora, tipo de transacción) Nombres y tamaños de los ficheros transferidos *Cookies*	Reunidos en el "fichero histórico común ampliado"
6. *Portales*	Información colectiva sobre las visitas a los sitios web correspondientes *Cookies*	Posibilidad de elaborar perfiles completos de los usuarios (datos sobre la comunicación y el comportamiento del usuario a disposición del *proveedor de servicios de Internet*)
7. Proveedores de servicios, incluidos los motores de búsqueda	Análisis de los registros recogidos en sitios web Datos y perfiles recogidos en sitios web a través de *cookies* Motores de búsqueda: palabras clave introducidas por el usuario de Internet	Ej.: NedStat Ej.: DoubleClick

III. Riesgos para la privacidad

Millones de usuarios de Internet de todo el mundo navegan con frecuencia por la World Wide Web o buscan información en Internet. Sin embargo, estas actividades no están exentas de riesgos desde el punto de vista de la privacidad.

En Internet se obtienen y tratan grandes cantidades de información de un modo que resulta invisible para el titular de los datos. En ocasiones, el usuario de Internet no es consciente de que sus datos personales se han recogido y procesado y se pueden utilizar con fines que ignora. El titular de los datos no está enterado del tratamiento y, por lo tanto, no es libre para decidir al respecto[81].

Además, cuando los datos recopilados durante la navegación por Internet pueden relacionarse con otras informaciones sobre el usuario, surgen otros riesgos. El temor a tal cruce de datos personales sobre usuarios de Internet ha estado muy presente en el debate sobre la fusión entre la empresa publicitaria de Internet DoubleClick y la empresa de estudios de mercado Abacus Direct.

[81] El Grupo de Trabajo del artículo 29 ya abordó esta cuestión en su Recomendación 1/99, adoptada el 23 de febrero de 1999: Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, adoptada por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17.

Se temía que, de producirse esta fusión, la base de datos de DoubleClick con información sobre los hábitos de uso de Internet pudiera cotejarse con la base de datos de Abacus Direct, que contenía nombres y direcciones reales, así como con información detallada sobre los hábitos de compra de los clientes[82].

La fusión se produjo en noviembre de 1999. De acuerdo con la información ofrecida en el sitio web de Doubleclick[83], los nombres y direcciones comunicados de forma voluntaria por un usuario en un sitio web perteneciente a Abacus Alliance serían cotejados por Abacus utilizando un código de correlación y la *cookie* de DoubleClick, con otras informaciones sobre el interesado.
La información contenida en la base de datos Abacus Online sobre cada usuario incluye: nombre, dirección, catálogo, historial de compras en línea y datos demográficos. Esta base de datos recoge igualmente información que no permite identificar a un usuario y que ha sido recabada por sitios web u otras empresas con las que DoubleClick mantiene relaciones comerciales.
Según DoubleClick, hasta la fecha no se ha establecido ninguna relación entre las bases de datos de DoubleClick y de Abacus.

Nuevo software de control

Los *proveedores de servicios de Internet* disponen actualmente de nuevas tecnologías de control que generarán una cantidad de información sobre modelos de tráfico y preferencias de contenido muy superior a la que ha existido en la red telefónica pública conmutada (PSTN). Estas tecnologías prometen ofrecer el equivalente en Internet de los registros de llamadas de la red telefónica pública conmutada, e incluso más.
El software de este tipo se conoce popularmente como aplicaciones E.T. *"porque, una vez que se han instalado en el ordenador del usuario y han aprendido lo que querían saber, hacen lo mismo que el extraterrestre de Steven Spielberg: llamar a casa"*[84].
A título de ejemplo, Narus, una empresa privada de software de Palo Alto, California (EE.UU.), ofrece a los *proveedores de servicios de Internet* software que "controla el flujo de datos y analiza cada paquete con objeto de extraer de él la cabecera e información útil"[85]. Narus afirma que trabaja en estrecha colaboración con socios clave, tales como Bull, Cisco y Sun Microsystems. Estos programas pueden utilizarse para identificar y medir la telefonía Internet y otras aplicaciones (como la Web, el correo electrónico o los faxes IP), pero también pueden controlar el contenido del tráfico IP que se puede facturar (por ejemplo, información protegida por derechos de autor que requiere el pago de un canon, el uso a medida de una aplicación o audioclips). Los programas de Narus informan en tiempo real al *proveedor de servicios de Internet* sobre los sitios web más visitados, así como sobre los contenidos visualizados y descargados[86].
Alexa[87] es una herramienta que puede añadirse a un navegador para acompañar al usuario durante la navegación y ofrecerle información adicional sobre el sitio visitado (titular registrado, valoraciones y análisis del sitio), así como hacerle sugerencias sobre sitios

[82] Véase EPIC Alert 6.10, 30 de junio de 1999. La misma preocupación surgió ya durante el caso de Harriet M. Judnick contra DoubleClick en el Tribunal Superior del Estado de California.
[83] www.doubleclick.net:8080/privacy_policy/ Esta fusión se analiza en detalle en el capítulo 7 sobre transacciones electrónicas en Internet.
[84] Véase el tema de portada de la revista Time del 31 de julio de 2000, de COHEN, Adam: *Cómo proteger tu intimidad: ¿quién te observa? Se llaman programas E.T. Te espían y "llaman a casa" para contarlo. Millones de personas los descargan de forma involuntaria.*
[85] http://www.narus.com
[86] Véase PALTRIDGE, Sam, *Mining and Mapping Web Content*, en: Info, *The Journal of policy, regulation and strategy for telecommunications, information and media*, vol. 1, nº 4, agosto de 1999, pp. 327-342.
[87] http://www.alexa.com

relacionados. A cambio de ofrecer este servicio a los usuarios, Alexa ha recabado una de las mayores bases de datos sobre hábitos de utilización de la Web. Amazon pagó 250 millones de dólares en acciones por Alexa a principios de los noventa. En su política de privacidad, Alexa afirma que la información recogida sobre la utilización de la Web a través de sus ficheros de uso de la misma y de *cookies* permanece anónima.

Otro de los productos fabricados por Alexa es el programa zBubbles, una herramienta de compra en línea que recoge datos de navegación sobre el usuario con objeto de ofrecerle recomendaciones sobre determinados productos, asesoramiento comparativo para sus adquisiciones, etc. De acuerdo con la información publicada en la revista Time[88], zBubbles también envía información a Alexa cuando los usuarios no compran. Este producto se ha diseñado para que aparezca en pantalla durante toda la sesión de navegación, aunque la mayoría de los usuarios no están comprando continuamente.

Otro ejemplo interesante de software de control es Radiate, antes conocido como Aureate. Radiate es una empresa publicitaria que trabaja con fabricantes de *software compartido*. Parece ser[89] que los anuncios de Radiate contenían software E.T. que se instaló en los ordenadores de 18 millones de personas, y utilizaron su conexión a Internet para obtener información sobre el tipo de anuncios que los usuarios visitaban en la Red. La versión original de los programas de Radiate, que aún reside en numerosos ordenadores, se desarrolló para seguir llamando a casa incluso después de que se borrase el programa de *software compartido* que la instaló en ellos. Los usuarios necesitaban una herramienta especial para eliminar el fichero que más adelante la empresa proporcionó desde su sitio web.

En la actualidad existen cientos de aplicaciones E.T. Se cree que más de 22 millones de personas las han descargado[90]. El software de control E.T. constituye de nuevo un ejemplo de tecnología de tratamiento de los datos personales de los usuarios sin que éstos se enteren (tratamiento invisible): la mayoría de los usuarios ni siquiera se imagina que estos programas están instalados en su ordenador.

A menudo, los fabricantes de estas aplicaciones E.T. declaran que aunque tienen capacidad para recoger datos relativos a los usuarios de los ordenadores no establecen conexiones con individuos. Sin embargo, esto no es una garantía suficiente para el usuario, pues, dado el valor comercial de los datos individualizados, las empresas que los recaban podrían modificar sus políticas en cualquier momento. El riesgo potencial de abuso de los datos sigue existiendo[91].

IV. Análisis jurídico

El punto de partida en el análisis jurídico de los fenómenos de navegación y búsqueda en Internet es que las dos Directivas sobre protección de datos (Directiva 95/46/CE y Directiva 97/66/CE) son, en principio, aplicables a Internet[92].

[88] Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.)*.
[89] Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.)*.
[90] Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.)*.
[91] Mencionado en el artículo de COHEN, A., en la revista Time *(op. cit.)*.
[92] Véase WP 16, Documento de trabajo: *Tratamiento de datos personales en Internet*, aprobado por el Grupo de Trabajo el 23 de febrero de 1999, 5013/99/ES/final.

Principales preceptos de la Directiva general 95/46/CE: principio de finalidad, tratamiento leal e información al interesado

Tres de las cuestiones abordadas en la Directiva general merecen una atención especial en este capítulo: el principio de finalidad, el principio de tratamiento leal y la información al interesado.

Información al titular de los datos

En Internet los datos fluyen con gran rapidez y a menudo no se observan las normativas tradicionales referentes a la información que se proporciona al interesado sobre el tratamiento de sus datos y los fines del mismo. En algunos casos, los usuarios de Internet no tienen pleno conocimiento de la existencia ni de las capacidades del software o el hardware a través de los que se realiza el tratamiento, como las *cookies* o las aplicaciones informáticas E.T.

El Grupo de Trabajo trató estos casos en su Recomendación 1/99[93], en la que destacó que el requisito de informar al titular a fin de que tenga conocimiento del tratamiento de sus datos constituye una condición para la legitimidad de éste. Los productos de hardware y software de Internet deberían proporcionar a los usuarios información sobre los datos que pretenden recabar, almacenar o transmitir, así como sobre el fin con que se han pedido.
Los productos de hardware y software de Internet también deberían permitir al interesado acceder fácilmente a los datos recabados sobre él con posterioridad.
El incumplimiento de las obligaciones impuestas por la Directiva general no se puede imputar a la velocidad de los flujos de datos en Internet. De hecho, Internet es un medio que permite ofrecer información rápida y sencilla al titular de los datos. Siempre que se recopilen datos de carácter personal, se debería proporcionar al interesado información básica[94] de un modo que garantice la recogida leal de sus datos, que podría ser, dependiendo de la situación, directamente en la pantalla o en el formulario en el que se obtienen los datos o a través de una casilla de aviso en la pantalla (por ejemplo, cuando se envían *cookies*). El interesado debería disponer de la posibilidad de oponerse al tratamiento u obtener más información haciendo clic en algún lugar.
Algunos sitios web siguen una política de privacidad que incluye la información sobre los datos que tratan, los fines de dicho tratamiento y la forma en que el interesado puede ejercer sus derechos. Sin embargo, ésta no es la regla general, y ni siquiera cuando existe tal política se ofrece toda la información necesaria.

Pese a estar a favor de las políticas de privacidad completas y precisas, el Grupo de Trabajo es claramente partidario de que se informe al interesado directamente en la pantalla o a través de la utilización de casillas de aviso en el momento en que se recopilan sus datos, sin que él tenga que realizar ninguna acción para acceder a la información, pues los usuarios de Internet no siempre leen las medidas de protección de la privacidad de todos los sitios web que visitan mientras navegan.

Para desempeñar un papel informativo serio, sería aconsejable que las descripciones de las medidas de protección de la privacidad no fuesen demasiado extensas, que presentasen una estructura clara y que ofreciesen información precisa sobre la política de protección de datos del sitio de forma sencilla y comprensible. El trabajo de la OCDE en

[93] Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, adoptado por el Grupo de Trabajo el 23 de febrero de 1999, 5093/98/ES/final, WP 17.
[94] La información debería incluir, al menos, detalles sobre el responsable del tratamiento, los fines del mismo y, si procede, el derecho a oponerse a él.

este campo (generador de políticas de protección de la privacidad o asistente en materia de privacidad), podría ayudar a alcanzar estos objetivos, aunque el uso de un generador no constituye por sí mismo una garantía de cumplimiento de las Directivas comunitarias.

En la práctica es improbable que las medidas de protección de la privacidad basten por sí mismas, pues no contienen información suficiente desde el punto de vista de la protección de datos. Un estudio reciente realizado por el EPIC[95] en Estados Unidos sobre las medidas de protección de la privacidad de los 100 sitios de comercio electrónico más visitados mostró que pocos de los sitios con tráfico intenso ofrecían una protección adecuada. De hecho, ninguno de ellos respetaba elementos importantes de las prácticas leales de información investigadas en el estudio[96].

Principio de finalidad

La información que se ha de proporcionar al titular de los datos debería ser, en todos los casos, suficiente y sencilla en lo que respecta a los fines del tratamiento. El artículo 6 de la Directiva general prohíbe que los datos sean tratados posteriormente de manera incompatible con dichos fines.

Este principio resulta especialmente relevante para los sitios web que recaban información sobre el comportamiento de navegación de los usuarios de Internet, para los programas a los que el usuario ha autorizado a controlar su comportamiento en Internet con un fin específico pero no con otros fines (desconocidos) y para los *proveedores de servicios de Internet*.
En principio, sólo los *proveedores de servicios de Internet* deberían recopilar datos de navegación relativos a los usuarios de Internet, y en la medida en que los necesiten para prestar un servicio al abonado, en este caso la visita a los sitios web que éste desee. En ocasiones, los *proveedores de servicios de Internet* mencionan la necesidad de conservar estos datos con el fin de poder supervisar el funcionamiento de sus sistemas. Sin embargo, ello no requiere el almacenamiento de datos que permitan la identificación del usuario, pues se puede medir y controlar el funcionamiento de un sistema basándose en datos agregados.

Un informe reciente de la Registratiekamer[97] concluyó que cuando los *proveedores de servicios de Internet* conservan datos individuales sobre tráfico de los usuarios no lo hacen en calidad de proveedores de acceso. Esta información resulta especialmente interesante para sus actividades como proveedores de contenido. Sin embargo, debería señalarse que éste es un fin completamente diferente.

Resultaría útil que el principio de limitación de los fines pudiera integrarse en medios técnicos. Esto podría considerarse también una forma de tecnología en favor de la protección de la privacidad[98].

Tratamiento leal de datos

El artículo 6 de la Directiva general contiene varios principios destinados a garantizar el tratamiento leal de los datos de carácter personal. Uno de ellos es el principio de limitación de los fines mencionado en los párrafos anteriores.

---

[95] Estudio "*Surfer Beware III: Privacy Policies Without Privacy Protection*", véase EPIC Alert 7.01, 12 de enero de 2000. Disponible en: www.epic.org/reports/surfer-beware.html.
[96] En EE.UU., las Prácticas leales de información sirven como directrices básicas para proteger la información personal.
[97] *Klant in het web: Privacywaarborgen voor Internettoegang (op. cit.).*
[98] Véase el capítulo 9.

Dicho artículo especifica igualmente que los datos de carácter personal deberían conservarse en una forma que permita la identificación de los interesados durante un período no superior al necesario a los fines para los que se han recogido. Esto significa que, una vez que los datos son anónimos para impedir que se puedan relacionar con el titular de los datos, pueden utilizarse con otros fines, como evaluar los resultados del servicio ofrecido por un *proveedor de servicios de Internet* o elaborar un estudio sobre el número de visitantes de un sitio web.

Los motores de búsqueda más utilizados mantienen registros de consultas en los que se recogen tanto las consultas como otros tipos de información, incluidos los términos utilizados[99]. Estos términos son interesantes para empresas que pretenden seleccionar *metaetiquetas* de páginas web y estimar la demanda en línea de contenidos relacionados con determinadas marcas, empresas o productos. Si no existe una relación entre el registro de la consulta y la identidad del usuario de Internet que introdujo la palabra clave, no existen obstáculos jurídicos que puedan impedir el mantenimiento de estos datos agregados.

Si los datos de navegación y búsqueda en Internet no se hacen anónimos, no deberían conservarse una vez finalizada la sesión de Internet. Esta cuestión se explicará con mayor detalle cuando se aborde la Directiva específica relativa a la intimidad y las telecomunicaciones en los datos sobre tráfico.

Al considerar la lealtad del fin del tratamiento de datos, también debería tenerse en cuenta el artículo 7 de la Directiva, que establece varias condiciones para que el tratamiento sea leal, incluidos el consentimiento del interesado y el equilibrio entre el interés legítimo del responsable de los datos y los derechos fundamentales del titular de los mismos. El responsable del tratamiento debería tener siempre en cuenta este equilibrio de intereses cuando recaba información personal de un usuario de Internet.

Principales preceptos de la Directiva específica sobre intimidad y telecomunicaciones

Como se puede observar en la tabla que aparece en el capítulo 3, algunas disposiciones de la Directiva de telecomunicaciones resultan especialmente pertinentes para la navegación y la búsqueda en Internet.

Aunque el título de la Directiva 97/66/CE se refiera al sector de las telecomunicaciones en general, es evidente que la terminología empleada en el texto se basa en la tecnología RDSI. La mayoría de los preceptos de esta Directiva utilizan términos como "llamadas", que aluden a la telefonía tradicional y RDSI y dificultan la aplicación a los servicios de Internet. No obstante, normalmente éstos se pueden incluir en el ámbito de aplicación de la Directiva, aunque, como se puede ver en los párrafos siguientes, se han de afrontar ciertas dificultades.

Sin embargo, muchos de estos problemas terminológicos quedan resueltos en el texto de la propuesta de revisión de la Directiva de 12 de julio de 2000[100], en el que se han actualizado algunas de las definiciones para garantizar la cobertura de todos los tipos diferentes de servicios de transmisión para las comunicaciones electrónicas, independientemente de la tecnología empleada.

Las referencias al término "llamadas" se limitan actualmente a los casos en que el legislador se refiere específicamente a llamadas telefónicas, tal como se especifica con la

[99] Véase PALTRIGDE, S., *Search engines and content demand,* in *Mining and Mapping Web Content*, en: *Info, The Journal of policy, regulation and strategy for telecommunications, information and media,* vol. 1, nº 4, agosto de 1999, pp. 330-333.
[100] COM (2000) 385.

inclusión de una definición de esta palabra en la letra e) del artículo 2[101]. En cualquier otro caso, el nuevo texto utiliza "comunicaciones" o "servicios de comunicaciones".

En los siguientes párrafos se comentarán las normas más pertinentes de la Directiva 97/66/CE. Siempre que resulte adecuado, este documento se referirá a los cambios introducidos por la nueva propuesta de revisión de la Directiva.

Artículo 4: Seguridad

Los proveedores de servicios de telecomunicación deberían ofrecer medidas adecuadas de seguridad que tomen en consideración las técnicas más avanzadas. Estas medidas deberían ser proporcionales a los riesgos de cada situación específica.

Este precepto resulta especialmente pertinente para los proveedores de *encaminadores* y líneas de conexión, ya que estos sistemas transportan grandes cantidades de información.

Este artículo no se ha modificado en la nueva propuesta, excepto en lo que respecta a la sustitución del término "servicios de telecomunicaciones" por "servicios de comunicaciones electrónicas".

Artículo 5: Confidencialidad

Las normas nacionales garantizarán la confidencialidad de las comunicaciones. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de interceptación o vigilancia de las comunicaciones por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados[102].

Son varios los agentes participantes en las actividades de búsqueda y navegación en Internet a los que afecta este artículo: proveedores de *encaminadores* y líneas de conexión, *proveedores de servicios de Internet* y proveedores de telecomunicaciones en general.

En principio, este artículo se refiere al contenido de la comunicación. Sin embargo, la distinción entre datos sobre tráfico y contenido no resulta fácil de aplicar en el contexto de Internet, sobre todo cuando se hace referencia a la navegación. En un primer momento, los datos relativos a ésta podrían considerarse datos sobre tráfico. No obstante, el Grupo de Trabajo opina que navegar por distintos sitios podría considerarse una forma de comunicación y, como tal, debería quedar cubierta por el ámbito de aplicación del artículo 5.

Por sí mismo, el comportamiento de navegación de un usuario de Internet (datos de navegación) que visite distintos sitios web puede revelar mucho sobre la comunicación que está teniendo lugar. En la mayoría de los casos, conociendo los nombres de los sitios web visitados se puede obtener una idea bastante precisa de la comunicación que se ha producido. Además, a quien posea los datos sobre tráfico le resulta sencillo visitar el sitio y ver exactamente los contenidos a los que se accedió.

Así pues, el Grupo de Trabajo considera que los datos de navegación de un usuario de Internet deberían recibir la misma protección que los contenidos. Por consiguiente, esta forma de comunicación debería ser confidencial. En este sentido, se puede considerar que las *series de clics* quedan dentro del ámbito de aplicación de este artículo.

[101] "Llamada" se referirá a una conexión establecida por medio de un servicio telefónico disponible al público que permita la comunicación bidireccional en tiempo real.

[102] A este respecto, véase la Recomendación 2/99 sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones, adoptada el 3 de mayo de 1999, 5005/99/final, WP 18.

En la letra c) del apartado 1 de su artículo 2, la nueva propuesta de revisión de la Directiva recoge la definición de "datos sobre tráfico": *(se entenderá por) "datos sobre tráfico", cualquier dato tratado en el curso de o a efectos de la transmisión de una comunicación a través de una red de comunicaciones electrónicas*. Por lo tanto, los datos de navegación quedarían incluidos en esta definición y se considerarían datos sobre tráfico.

La revisión de esta Directiva ha entrañado otras mejoras gracias a la ampliación del ámbito de aplicación del artículo 5 para abarcar no sólo el contenido de la comunicación, sino también los datos sobre tráfico correspondientes. Al ofrecer la misma protección al contenido que a los datos sobre tráfico relacionados con él se resta importancia a la distinción, no siempre evidente, entre estos conceptos. El Grupo de Trabajo acoge favorablemente esta mejora.

Artículo 6: Tráfico y facturación

Los datos sobre tráfico deberán destruirse o hacerse anónimos en cuanto *termine la comunicación*. Con objeto de interpretar este artículo en el contexto de Internet es necesario definir lo que puede considerarse datos sobre tráfico y lo que puede entenderse por contenido de la comunicación.

Este artículo parece guardar una estrecha relación con las telecomunicaciones por conmutación de circuitos que conectan a dos o más partes de la comunicación. Los datos sobre tráfico se crean en el proceso de establecimiento y mantenimiento de esta conexión, lo que dificulta especialmente la aplicación de este artículo en el contexto de Internet.

En el tráfico de Internet, los paquetes que se transmiten están "envueltos" en varias cabeceras de *protocolos*, tales como la cabecera TCP, la cabecera IP y la cabecera Ethernet. Estas cabeceras de *protocolos* se leen en cada uno de los nudos (*encaminadores*) que atraviesa un paquete para decidir a dónde se dirigirá el siguiente envío de dicho paquete. Sin embargo, no parece necesario que cada nudo intermedio almacene datos de las cabeceras una vez que ha transmitido el paquete.

La información contenida en las cabeceras, que puede incluir datos sobre el contenido de los paquetes, se debería considerar datos sobre tráfico en el sentido del artículo 6 de la Directiva 97/66/CE y, por tanto, se debería tratar de forma anónima o borrarse una vez que estos datos ya no sean necesarios para el mantenimiento de la comunicación, es decir, tan pronto como el usuario de Internet acceda al sitio web.

No cabe duda de que algunos datos como los referentes a la conexión de la sesión (hora de conexión y desconexión, cantidad de datos transferidos, hora de inicio y fin de la sesión, etc.) deberían incluirse en el ámbito de aplicación del artículo 6.

La lista de sitios web visitados por un usuario de Internet (comportamiento de navegación) debe considerarse en cualquier caso datos sobre tráfico (y puede ser objeto de la misma protección que el contenido). Sobre todo, esta lista debería destruirse en principio *en cuanto termine la sesión de Internet*.

Resulta interesante señalar que el ordenador personal conserva siempre un registro de las actividades de navegación del usuario de Internet. Esto puede ser un problema cuando varios usuarios comparten un ordenador.

En el pasado, el Grupo de Trabajo emitió dictámenes sobre la cuestión de los *proveedores de servicios de Internet* que almacenan datos sobre tráfico con fines de

cumplimiento de la ley[103]. Esta Recomendación establece que, en principio, los datos sobre tráfico que no sean necesarios para la facturación no deberían conservarse. En el caso de *proveedores de servicios de Internet* gratuitos no sería necesario guardar datos sobre tráfico, ya que, al no requerirlos para la facturación, no habría necesidad de ellos una vez concluidas las operaciones normales.

La Directiva revisada sustituye la expresión "en cuanto termine la comunicación" por "en cuanto concluya la transmisión", que resulta más clara. Por lo tanto, los datos sobre comportamiento de navegación deberían eliminarse una vez finalizada la conexión a Internet.

El nuevo texto introduce la posibilidad de un tratamiento posterior para prestar servicios de valor añadido o para comercializar servicios propios de comunicación electrónica si el abonado ha dado su consentimiento. Sin embargo, el término "servicio de valor añadido" no se define en la propuesta. El Grupo de Trabajo considera necesario aclarar qué debería incluir esta definición para garantizar la limitación de los fines y reducir los nuevos riesgos para la privacidad. Del mismo modo, el Grupo de Trabajo recomienda que se incluya una "prueba de necesidad" relativa a la posibilidad de tratar datos sobre tráfico para las actividades comerciales propias del proveedor[104].

Artículo 8: Identificación de la línea llamante y la línea conectada

En Internet no hay líneas llamantes que identificar. No hay un canal de encaminamiento separado que permita establecer la identidad de quien realiza la llamada antes de que se establezca la conexión.

En Internet, la dirección IP no se puede separar de la comunicación (los paquetes), por lo que el concepto de *identificación de la línea de llamada* no se puede aplicar directamente.

Técnicamente hablando, no es posible ofrecer servicios de telecomunicación relacionados con Internet sin transmitir y utilizar la dirección IP que el usuario ha empleado durante una sesión.

Por tanto, se puede concluir que el artículo 8 de la Directiva de telecomunicaciones no puede aplicarse a las direcciones IP del mismo modo que se aplica a los números de teléfono.

La propuesta de revisión de la Directiva de 12 de julio de 2000 sigue esta línea de pensamiento. La redacción de este artículo se mantiene prácticamente inalterada y sigue utilizando el término "llamada", un concepto que en el nuevo texto se reserva a los servicios de telefonía.

V. Medidas en favor de la privacidad

La protección real de la privacidad mientras se navega por Internet se puede garantizar de diversas formas. Presentamos aquí algunas opciones para aumentar el grado de protección de la privacidad del usuario[105].

En primer lugar, muchos métodos de recopilación de datos personales se basan en el uso de *cookies*. Los programas de navegación que emplea el usuario de Internet permiten

[103] Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación, aprobada el 7 de septiembre de 1999, 5085/99/ES/final WP 25.
[104] Véase el Dictamen 7/2000 del Grupo de Trabajo, adoptado el 2 de noviembre de 2000, WP 36.
[105] Para más detalles, véase el capítulo 9 sobre medidas en favor de la privacidad.

impedir la instalación de éstas en su disco duro, ya sea de forma individual o de modo sistemático. Sin embargo, cabe señalar cada vez son más numerosos los sitios web que sólo ofrecen un servicio completo si se autorizan las funciones de la *cookie*.

El 20 de julio de 2000 Microsoft anunció que la próxima versión de Internet Explorer incluiría la versión beta de un sistema de seguridad que permitiría una mejor gestión de las *cookies* de web[106]. La versión de prueba debería estar a disposición del público a finales de agosto.
De acuerdo con la información previa, dicho sistema presentará varias características que permitirán a los usuarios controlar las *cookies* de forma más eficaz. El navegador podrá diferenciar entre las *cookies* procedentes del interlocutor de la comunicación y las procedentes de terceros, y la instalación por defecto avisará al usuario cuando se esté instalando una *cookie* duradera procedente de éstos. Las empresas publicitarias de Internet, como DoubleClick o Engage, recurren con mucha frecuencia a estas *cookies* procedentes de terceros para seguir la pista de las actividades de los usuarios. Además, la nueva función permitirá al usuario eliminar todas las *cookies* con un simple clic y facilitará el acceso a información sobre seguridad y privacidad. Sin embargo, este sistema de seguridad no aumentará el control del consumidor sobre el uso de *cookies* procedentes del interlocutor principal, muy habituales en sitios web comerciales.
El diseño de las características de gestión de las *cookies* va pisando los talones al de otros sistemas de seguridad creados recientemente por Microsoft para solucionar problemas de fuga de datos. En mayo de 2000, la empresa presentó una extensión del popular programa Outlook capaz de suprimir las *cookies* de los mensajes de correo electrónico.
Sin embargo, resulta lamentable que esta tecnología no permita todavía al sitio que origina la *cookie* indicar inmediatamente el fin con que ésta se utilizará.

En segundo lugar, el *proveedor de servicios de Internet* puede contribuir a la protección de la privacidad del usuario de Internet limitando los datos personales almacenados al mínimo necesario para el establecimiento de la conexión y el mantenimiento del funcionamiento técnico. En particular, en muchos casos el *proveedor de servicios de Internet* puede ocultar a un sitio web el número IP de un usuario de Internet mediante una conexión con dicho sitio desde un *servidor proxy* especial. En ese caso, sólo se transmite el número IP asignado por el *servidor proxy*, mientras que el *proveedor de servicios de Internet* conserva la dirección del usuario de Internet. Sin embargo, éstos servicios no se suelen ofrecer de modo estándar.

En tercer lugar, algunos *portales* pueden actuar como *organismos de confianza* que custodian los datos personales del usuario. Estos "informediarios" pueden actuar como vigilantes que sólo suministran datos de carácter personal a sitios web que respetan la privacidad del usuario de Internet, o pueden "negociar" con la información personal de que disponen para conseguir determinados beneficios, siempre que el titular esté al corriente de ello y haya dado su consentimiento[107]. Sin embargo, esta última opción debería considerarse con precaución.

El método que garantiza mayor rigor al usuario de Internet es la elección de servicios que ocultan de forma intencionada su dirección IP a los sitios web que visita. Determinados programas y sitios web permiten mantener en el anonimato las direcciones IP de los usuarios redireccionando la comunicación a través de servidores dedicados que sustituyen la dirección IP por otra.

La existencia de nuevos programas que controlan el software E.T. hace que se vuelvan a plantear cuestiones sobre las posibles medidas de protección. Un método de protección

[106] EPIC Alert 7.14, 27 de julio de 2000.
[107] Para más detalles, véase el libro *Net Worth (op. cit.)*.

posible[108], aunque difícil de llevar a la práctica, consistiría en la segmentación física de los discos duros de los ordenadores en una parte pública y otra privada, de forma que los datos descargados no pudieran acceder a la información que se desee mantener confidencial. En cualquier caso, se recomienda ser extremadamente prudente al descargar aplicaciones procedentes de Internet o del correo electrónico.

VI. Conclusiones

- Es necesario ofrecer acceso anónimo a Internet a los usuarios que navegan o realizan búsquedas en la Red, por lo que se recomienda vivamente el uso de *servidores proxy.*
- El uso cada vez mayor de software de control es una tendencia que debería tomarse en consideración y recibir la atención debida, pues puede tener graves consecuencias en la privacidad de los usuarios de Internet.
- Ciertas definiciones y algunos conceptos utilizados en la redacción actual de la Directiva de telecomunicaciones no resultan fáciles de aplicar a los servicios relacionados con Internet.

  - La diferenciación tradicional entre contenido y datos sobre tráfico no puede aplicarse fácilmente a las actividades de Internet, sobre todo en lo que respecta a la navegación: por una parte, el concepto de datos sobre tráfico debería interpretarse de forma amplia para incluir los datos contenidos en cabeceras y todos los datos de conexión; por otra, debería ofrecerse a los datos sobre comportamiento de navegación el mismo grado de protección que a los referentes al contenido.

  - Las normas relativas a la *identificación de la línea llamante* deberían revisarse en el contexto de Internet.
- La revisión de esta Directiva ha provocado un gran avance en el primero de estos puntos gracias a la ampliación del ámbito de aplicación del artículo 5 con objeto de cubrir no sólo el contenido de la comunicación, sino también los datos sobre tráfico con él relacionados, y ofrecer así la misma protección a ambos. El Grupo de Trabajo acoge favorablemente esta mejora. El segundo problema también ha quedado resuelto tras aclarar que este precepto sólo se aplica a las llamadas telefónicas y no a Internet.

  Con la revisión, la terminología se ha adaptado al nuevo contexto ampliado, lo que ha aclarado enormemente la Directiva y ha facilitado la interpretación de las disposiciones vigentes. No obstante, el Grupo de Trabajo desearía señalar que el concepto de "servicios de valor añadido" precisa una mayor especificación con objeto de evitar una interpretación demasiado amplia.

[108] Así lo sugirió Cheswick, investigador jefe de Lucent technologies, en el artículo de COHEN, A., en la revista Time *(op. cit.)*.

CAPÍTULO 6: PUBLICACIONES Y FOROS

I. Introducción

Las publicaciones y los foros disponibles en Internet tienen en común que en ellos se hacen públicos datos de carácter personal, ya sea con la participación del interesado, como sucede en los foros de debate públicos, ya sin ella, como en las guías. Los motivos por los que se publican estos datos personales son muy diversos. El usuario de Internet puede comunicar cierta información porque así se le ha solicitado, por ejemplo, para poder entrar en una sala de charla, o puede suceder que sea un tercero quien publique los datos, como en el caso de un organismo público, con fines administrativos.
La cuestión principal que plantea esta difusión de información es la aplicación de los principios de privacidad a los datos públicamente disponibles en la Web. En contra de lo que se piensa generalmente, la protección que ofrece la legislación sobre protección de datos se sigue aplicando a los datos publicados. En este capítulo se prestará especial atención a los motivos y las necesidades que llevan a la publicación de datos personales, al fin con que ésta se realiza y a los riesgos de abuso de los datos.

II. Descripción técnica

Foros públicos de debate

Los aspectos técnicos del tratamiento de datos en foros públicos de debate varían según la naturaleza de éstos. Se pueden distinguir dos tipos principales de foros: los de debate y la charla electrónica.

Foros de debate

Los grupos de discusión son foros clasificados por tema sobre el que los usuarios pueden presentar sus aportaciones y respuestas, para lo cual todos los datos enviados por los usuarios se almacenan durante un determinado período de tiempo.

Toda cuestión o artículo consta de un "título" y de un "cuerpo". El enlace entre un artículo y la respuesta al mismo es un "hilo".

En la transmisión de los mensajes a los servidores de foros de debate se utilizan *protocolos* específicos. El *protocolo* habitual de tratamiento de noticias es el NNTP (*protocolo* de transferencia de noticias a través de la red), aunque algunos foros utilizan también el *protocolo* HTTP. El NNTP procesa conexiones permanentes entre servidores de foros de debate y actualiza automáticamente los mensajes. El servidor del foro de debate almacena estos mensajes en un disco duro que cualquier persona conectada puede consultar. Las noticias se presentan en formato HTML.

Cada servidor compara con los demás su lista de artículos en cada foro de debate e intercambia con ellos nuevos artículos. Este proceso produce millones de intercambios de datos en Internet.

Dado el gran número de foros existentes, los usuarios sólo almacenan una lista reducida de ellos, debido a su gran número, y los programas de consulta sólo presentan los títulos de los artículos nuevos y dejan a iniciativa del interesado la descarga del texto del documento.

Charla electrónica

Existen tres tipos principales de charla en Internet: la charla interactiva Internet (IRC),la charla de página web (*Java*) y la charla ICQ ("I seek you" – te busco).

1. La charla interactiva Internet (IRC) es el modo original de charla electrónica. Utiliza un *protocolo* que permite a los usuarios comunicarse en tiempo real, ya sea públicamente, en un foro con un número indeterminado de personas, o en privado, con un único interlocutor. Al igual que los foros de debate, las salas de charla varían según los temas, pero se diferencian de éstos en que los canales se cancelan una vez concluido el debate.

Los retrasos en la transmisión de información en las principales charlas interactivas Internet han llevado a la creación de redes independientes, entre las que destacan EfNet, UnderNet y DalNet.

2. La charla de página web permite comunicarse sin necesidad de un programa separado: la única herramienta que se necesita es un navegador de Internet moderno. Existen dos tipos de charla de página web: la dedicada, disponible en la mayoría de los sitios de búsqueda de los *portales* de la Web, y la que el usuario instala en su propia página de inicio. Aunque la charla de página web resulta muy sencilla de utilizar, sus capacidades son limitadas: a diferencia de lo que sucede en la charla interactiva Internet (IRC), sólo permite intercambiar texto, y no modificar colores, enviar sonidos, mandar ni recibir ficheros, ejecutar scripts ni personalizar los elementos de la interfaz de charla.

3. La charla ICQ es una herramienta que informa al usuario que está continuamente en línea y le avisa cuando se conectan personas predefinidas (incluidas en una lista de contactos personales) y le permite contactar y charlar con ellas y enviarles mensajes mientras sigue navegando por la Red, siempre que todos los participantes estén utilizando ICQ. Se pueden dar instrucciones al programa para que señale al usuario como invisible, ausente o no disponible.

Publicaciones y guías

Normalmente, las publicaciones y las guías se publican en Internet en forma de bases de datos que ofrecen criterios de búsqueda para obtener información sobre una o varias personas.

Tradicionalmente, la fuente de información de las guías telefónicas es la guía oficial nacional que edita, según el país, el operador principal de telecomunicaciones o una empresa responsable de recabar los datos basándose en la lista de abonados.

Existen distintos medios de recopilación de listas de correo electrónico, desde la inscripción voluntaria de los usuarios de Internet en una lista que presenta un *proveedor de servicios de Internet*, a la recogida incontrolada de direcciones de correo electrónico en sitios web, tales como los foros de debate.

Existen otras publicaciones sobre diversos temas, como las listas editadas por organismos públicos, que pueden incluir, por ejemplo, la jurisdicción de un país con los datos de las sentencias, los tribunales, la situación e incluso los nombres de las partes y del juez, así como un resumen del caso.

La mayoría de las bases de datos existentes en Internet ofrecen varios criterios de búsqueda que permiten acceder a la información de forma personalizada y organizan los resultados de distintas formas. En una guía telefónica se podría iniciar una búsqueda a partir de un nombre o un número de teléfono, mientras que en una base de datos de jurisprudencia el criterio podría ser la fecha de una sentencia, el nombre de una de las partes, etc.

III. Riesgos para la privacidad

Foros públicos de debate

La accesibilidad a los datos de carácter personal comunicados por el usuario de Internet constituye el principal riesgo para la privacidad[109]. La posibilidad de acceder a estos datos puede dar lugar a su recogida y posterior utilización con fines que el participante en los foros públicos no siempre es capaz de prever con claridad. Por otra parte, el titular de los datos no siempre tiene conocimiento de los detalles que se publican habitualmente junto con el contenido de su aportación al foro.

En el caso de los foros de debate, por ejemplo, la dirección de correo electrónico del participante suele publicarse junto con su nombre o seudónimo[110]. Determinadas charlas electrónicas muestran, además del seudónimo del usuario que accede a ellas, la dirección IP de su ordenador. Algunos *proveedores de servicios de Internet* ofrecen la posibilidad de intervenir en un foro sin ser identificado por los demás participantes, pero también, por otro lado, la de acceder a la charla y que otros participantes lean un perfil específico del interesado.

La información de carácter personal disponible en línea varía según el foro. Como norma general, para dar acceso a un usuario a una sala de charla el *proveedor de servicios de Internet* le pide que cumplimente un cuestionario de identificación detallado que normalmente incluye la dirección de correo electrónico, la fecha de nacimiento, el país, el sexo y, en ocasiones, ciertas preferencias del usuario.

Sin embargo, desde el punto de vista técnico la comunicación de esta información detallada no es necesaria para el buen funcionamiento del foro de debate o de la charla, en el sentido del artículo 6 de la Directiva 95/46/CE.

Además, posteriormente esta información registrada podría ser utilizada por el *proveedor de servicios de Internet* y se podría combinar con detalles adicionales sobre el interesado recabados en línea en salas de charla.

Dos de los motivos principales para utilizar los datos recopilados o publicados son:

1. Controlar la naturaleza del contenido difundido. El objetivo de esta medida es garantizar que no se publiquen contenidos inadecuados y establecer la responsabilidad en caso de que se publiquen contenidos ilegales[111]. Con este fin, y para que el contenido siga siendo identificable, se suele guardar el rastro de los datos sin realizar una selección previa, independientemente del tipo de información aportada, aunque quizá fuese suficiente la dirección de correo electrónico y, tal vez, el nombre del participante.

2. Confeccionar listas de datos personales. Los datos personales se pueden recopilar en la Web con software capaz de buscar en la red y reunir todos los datos disponibles sobre una persona determinada. El Grupo de Trabajo incluyó en su Recomendación

[109] La Agencia Española de Protección de Datos ha tratado esta cuestión en su documento "Recomendaciones a los usuarios de Internet", disponible en español e inglés en su sitio web: www.agenciaprotecciondatos.org.

[110] Es frecuente que la primera parte de una dirección de correo electrónico coincida con el nombre del usuario, sobre todo cuando ha sido definida automáticamente por un proveedor de acceso a Internet a partir de su nombre registrado. Sin embargo, por lo general el usuario puede modificar esa parte de la dirección y utilizar, por ejemplo, un seudónimo. También se puede solicitar una segunda dirección; en este caso el proveedor de acceso permitirá al usuario elegir un nombre.

[111] Tal vez para impedir que la responsabilidad recaiga en el proveedor de servicios responsable del foro.

3/97[112] una cita de un artículo periodístico que explicaba *cómo se podría elaborar una biografía detallada de una persona seleccionada al azar utilizando estos programas y extraer información de todos los foros de debate en los que hubiera participado*, incluyendo datos como su dirección, su número de teléfono, su lugar de nacimiento, su lugar de trabajo, su destino favorito para las vacaciones y otros intereses personales. Estos datos podrían recopilarse y tratarse después con fines diversos, como la venta directa, pero también con objeto de conocer su solvencia crediticia o para venderlos a compañías de seguros o a empresarios. Algunos sitios web ya ofrecen herramientas de acceso público que permiten obtener todas las aportaciones que una persona ha realizado en foros de debate a partir de su nombre o su dirección de correo electrónico[113].

Publicaciones y guías

La disponibilidad en línea de información de carácter personal extraída de registros públicos o de otras fuentes de acceso público, tales como guías, plantea cuestiones similares a las mencionadas que están relacionadas con la posible utilización posterior de datos personales a escala mundial con un fin distinto de aquél para el que se publicaron originalmente[114].

Como ya se ha señalado, la informatización de los datos y la posibilidad de realizar búsquedas en textos completos ofrecen un número ilimitado de maneras de solicitar y clasificar información, y la extensión de Internet aumenta el riesgo de recopilación con fines inadecuados. Además, la informatización ha facilitado enormemente la combinación de datos de acceso público procedentes de distintas fuentes, lo que permite elaborar un perfil de la situación o el comportamiento de los usuarios. Por otra parte, se debería prestar especial atención a la utilidad de la publicación de datos de carácter personal como un modo de fomentar nuevas técnicas de *almacenamiento y minería de datos*[115]. Estas técnicas permiten recabar datos sin especificar previamente el fin y no definirlo hasta el momento en que se utilice efectivamente la información[116].

Se pueden mencionar varios casos concretos para ilustrar esta preocupación:

- Aunque las bases de datos de la jurisprudencia son instrumentos públicos de documentación jurídica, su publicación en formato electrónico en Internet, con criterios amplios de búsqueda de juicios, podría dar lugar a la creación de ficheros con información sobre individuos. Esto es lo que sucedería si se consultase una base de datos

[112] Recomendación 3/97 sobre anonimato en Internet, adoptada por el Grupo de Trabajo el 3 de diciembre de 1997.

[113] Véase, por ejemplo, el sitio Internet de Deja: "http://www.deja.com/home_ps.shtml?", que ofrece una "potente herramienta de búsqueda" con varios criterios de búsqueda, incluido el autor de mensajes en foros de debate. El sitio afirma que dispone de la mayor base de datos de la red sobre aportaciones a foros de debate.

[114] Con relación a este tema, véase la aportación del Sr. Marcel PINET, miembro de la CNIL, en la Conferencia internacional sobre protección de datos, celebrada en Santiago de Compostela en septiembre de 1998, disponible en: www.cnil.fr, en el apartado Internet, Initiatives.

[115] El *almacenamiento* y la *minería de datos* implican "excavar en toneladas de datos" para descubrir modelos y relaciones existentes, por ejemplo, en la historia y la actividad comercial de una organización. Se considera que el almacenamiento de datos debe prestar apoyo a la toma de decisiones. El tratamiento de la ingente cantidad de información se realiza con ayuda de software que permite una conexión sencilla entre informaciones relacionadas de la base datos. Véase el informe de la Registratiekamer (BORKING, J., ARTZ, M. y VAN ALMELO, L.), *Gouden bergen van gegevens: over datawarehousing, datamining en privacy*, Achtergrondstudies en verkenningen 10 de septiembre de 1998, disponible en: www.registratiekamer.nl.

[116] Dictamen n°3/99 relativo a información del sector público y protección de datos personales, aprobado por el Grupo de Trabajo el 3 de mayo de 1999.

con el fin de obtener una lista de sentencias judiciales sobre una persona en vez de localizar sólo un caso jurídico.

- También se puede obtener información concreta sobre una persona combinando los datos existentes en bases de datos electrónicas separadas. Por ejemplo, los nombres de las personas sin derecho a voto podrían recabarse cotejando los registros de población con los censos electorales.

- Generalmente, las guías de direcciones en Internet permiten buscar personas no sólo por su nombre, sino también por su dirección y su número de teléfono. Los interesados no prevén estas búsquedas inversas cuando dan su consentimiento para la publicación de su dirección en la guía telefónica en papel. La disponibilidad de los datos en formato electrónico significa que éstos podrían utilizarse con fines diversos, como la venta directa, seleccionando categorías de personas que viven en la misma zona (tal vez para vender sistemas de alarma en zonas residenciales), o la identificación y el registro de una persona que realiza una llamada a una empresa para lo que considera una sencilla solicitud anónima de información.

Las publicaciones en Internet pueden dar lugar a otras formas de recogida de información personal que se centrarían no sólo en los datos de carácter personal de una charla, un registro público o un directorio, sino también en información directa ofrecida en una página web personal. La indización automática de estas páginas realizada con robots de búsqueda puede hacer posible que se elaboren ficheros con información personal extraída de esas páginas, lo que a su vez posibilitaría la comercialización o el envío de *buzonfia* ("spam") dirigida al autor de dichas páginas o a las personas que hayan participado en ellas.

IV. Análisis jurídico

Foros públicos

Se ha previsto imponer obligaciones a los *proveedores de servicios de Internet* con el fin de limitar los riesgos de recogida ilícita de datos personales publicados en salas de charla o foros de debate.

La Recomendación nº R (99) 5 del Consejo de Europa relativa a la protección de la privacidad en Internet[117] establece para los *proveedores de servicios de Internet* la directriz de que informen a los usuarios, antes de que se abonen o empiecen a utilizar sus servicios, de los riesgos que el uso de Internet presenta para su privacidad. La información debe cubrir la *integridad de los datos*, la confidencialidad, la seguridad de la red y otros riesgos para la privacidad, como la recogida o la grabación invisible de datos.

El formulario de inscripción que los usuarios han de completar para solicitar acceso a un foro público debe respetar lo dispuesto en el artículo 6 de la Directiva 95/46/CE sobre el tratamiento leal de datos personales, que estipula que éstos deben recogerse con fines legítimos e impone la prohibición de recabar datos que no resulten necesarios ni pertinentes para dicho fin.

La legitimidad del fin puede determinarse sobre la base del artículo 7 de la Directiva 95/46/CE, que exige en particular el consentimiento explícito del titular para el tratamiento de sus datos personales, así como el equilibrio entre el interés legítimo del responsable del tratamiento y los derechos fundamentales del interesado (letras a y f del artículo 7).

[117] Recomendación del Comité de Ministros a los Estados miembros adoptada el 23 de febrero de 1999. Disponible en: www.coe.int/dataprotection/.

Se deberá informar a los usuarios de una forma clara y visible sobre el fin del tratamiento, la calidad de los datos recabados y el posible período de almacenamiento. Si esta obligación no se respeta, la falta de respuesta del usuario no se podrá considerar un consentimiento tácito para que el responsable de los datos realice un tratamiento posterior de éstos (por ejemplo, con fines comerciales).

Cabe destacar que los proveedores de servicios no necesitan conocer en todo momento la identidad del usuario. Antes de aceptar las suscripciones y de conectar a los interesados a Internet deberían informarles sobre la posibilidad de acceso anónimo o con un seudónimo y de utilización anónima de sus servicios[118].

El Grupo de Trabajo ha reconocido este principio en su Recomendación 3/97 sobre anonimato en Internet[119]. Aunque no cabe ninguna duda sobre la legitimidad del anonimato en situaciones como el intercambio de experiencias personales (alcohólicos o víctimas de abusos sexuales) o de opiniones políticas, el Grupo de Trabajo ha insistido en que la necesidad de anonimato en Internet va mucho más allá de estos casos concretos, *los datos transaccionales identificables crearán un medio a través del cual podrá observarse y controlarse la actuación de las personas en una medida que hasta ahora no había sido posible*.

El control de los foros de debate y las charlas electrónicas con objeto de prohibir contenidos inapropiados debería ejercerse de conformidad con el principio de proporcionalidad establecido en el artículo 6 de la Directiva 95/46/CE. En este sentido, la identificación y recopilación de los datos personales aportados en un foro público se considera desproporcionada en relación con otros medios de control existentes. Se han propuesto otras posibilidades, como soluciones contractuales que ofrecen "calidad de contenido" o la participación de un moderador encargado de supervisar las aportaciones para detectar contenidos dañinos o ilegales.

Junto con estos principios fundamentales, cabría añadir que la conservación de datos sobre tráfico por parte de los *proveedores de servicios de Internet* se ha regulado de forma muy estricta, al igual que en el caso de los operadores de telecomunicaciones. Como norma general, los datos sobre tráfico deben destruirse o hacerse anónimos en cuanto termine la comunicación (apartado 1 del artículo 6 de la Directiva 97/66/CE). Los operadores de telecomunicaciones y los *proveedores de servicios de Internet* no pueden recabar ni almacenar información sólo con fines de cumplimiento de la legislación, a menos que así se lo exija la ley por motivos concretos y en condiciones específicas[120].

Publicaciones y guías

El Grupo de Trabajo ha reiterado[121] que la legislación europea sobre protección de datos se aplica a los datos personales de acceso público y que la protección de esos datos sigue siendo necesaria.

El principio fundamental aplicable a los datos públicos de carácter personal es el de finalidad o limitación de los fines, en virtud del cual los datos personales sólo se pueden recabar con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines (letra b) del apartado 1 del artículo 6 de la Directiva 95/46/CE).

---

[118] S. LOUVEAUX, A. SALAÜN, Y. POULLET, *User protection in the cyberspace: some recommendations*, CRID, p. 12, disponible en: http://www.droit.fundp.ac.be/crid/.

[119] Recomendación adoptada por el Grupo de Trabajo el 3 de diciembre de 1997.

[120] Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los *proveedores de servicio Internet* a efectos de cumplimiento de la legislación, aprobada por el Grupo de Trabajo el 7 de septiembre de 1999.

[121] Dictamen n°3/99. Véase más arriba.

El Grupo de Trabajo ha subrayado igualmente que los datos personales puestos a disposición del público no constituyen una categoría homogénea que pueda tratarse de manera uniforme desde el punto de vista de la protección de datos: el acceso público a los datos puede existir pero estar sujeto a ciertas condiciones, tales como la prueba del interés legítimo, y a restricciones de su uso posterior, como el uso con fines comerciales.

La publicación de datos personales en Internet podría dar lugar a un tratamiento posterior de los datos no previsto por el interesado. Los artículos 10, 11 y 14 de la Directiva 95/46/CE establecen a este respecto que el titular tiene derecho a recibir información sobre la utilización de sus datos personales. Además, ha de ser informado sobre su derecho a oponerse al tratamiento de datos personales con fines comerciales por medios sencillos y eficaces.

La idea de una "ventanilla única" para oponerse al tratamiento de datos personales por medio de una lista única puede constituir una solución interesante para las dificultades que los usuarios encuentran a la hora de evitar una operación de tratamiento de datos, dado el gran número de ellas que existen tanto a escala nacional como en el ámbito internacional[122].

Si el fin previsto para el tratamiento resulta incompatible con el propósito original, el equilibrio entre el derecho a la intimidad y los intereses del responsable de los datos se logrará con la imposición de condiciones más estrictas a éste, que deberá solicitar el consentimiento del titular de los datos o demostrar que existe un fundamento jurídico o reglamentario para el tratamiento.

Sin embargo, no siempre queda claro si el responsable está obligado a respetar el derecho de oposición del titular o a solicitar su consentimiento a la hora de tratar sus datos.

La reglamentación de las guías de Internet en los distintos países es un ejemplo de la diversidad de enfoques. La cuestión radica en si es necesario el consentimiento previo cuando la publicación en formato electrónico de un directorio presenta criterios de búsqueda diferentes de los previstos originalmente en el directorio en papel.

Algunos países, como España y Bélgica, consideran que la ampliación de los criterios de búsqueda ofrece la posibilidad de tratar datos personales con fines incompatibles con el propósito original y que este tratamiento no debería autorizarse sin informar previamente al interesado y solicitar su consentimiento. En otros países, como el Reino Unido, en principio el cumplimiento del derecho a oponerse previsto en la Directiva parece considerarse suficiente, aunque dependerá de si existe o no obligación jurídica de publicar la información en la guía.

Estas interpretaciones de los textos jurídicos provocan diferencias en el grado de protección existente en los distintos países de la UE y conflictos prácticos cuando, por ejemplo, se publica en Internet una guía con datos personales de ciudadanos de un país en el que existe un grado elevado de protección desde otro en el que la política de protección es más permisiva.

Estos conflictos se han debatido a escala europea y la interpretación común que el Grupo de Trabajo ha hecho de los textos ha dado lugar a una posición oficial que recomienda la aplicación armonizada del principio en todos los Estados miembros de la UE[123].

[122] Esto podría resultar especialmente útil en lo que respecta a la difusión de guías en Internet. A menudo, las reclamaciones gestionadas por las autoridades de protección de datos se basan en la publicación de datos desde un determinado país cuando el afectado se ha registrado en una lista de oposición, pero sólo en su propio país.

[123] Dictamen 5/2000 sobre el uso de las guías telefónicas públicas para servicios de búsqueda inversa o multicriterio (guías inversas), WP 33, adoptado el 13 de julio de 2000.

El artículo 12 de la propuesta de revisión de la Directiva 97/66/CE[124] establece el derecho de los abonados a determinar sin coste alguno si aprueban la incorporación de sus datos y cuáles de ellos podrán aparecer en guías públicas, con qué fin concreto y en qué medida. Esto constituye un avance en la dirección correcta y ha recibido el apoyo absoluto del Grupo de Trabajo.

V. Medidas en favor de la privacidad

Además de las disposiciones jurídicas mencionadas, existen soluciones técnicas que pueden aumentar la protección de los datos personales a distintas escalas.

Como principio general, el Grupo de Trabajo señala que los programas de navegación deberían configurarse por defecto de manera que sólo se trate la cantidad mínima de información necesaria para establecer la conexión a Internet[125].

Anonimato en foros públicos

Con relación al anonimato en Internet, y en particular en los foros públicos, la idea de la "seudoidentidad" podría ofrecer una solución alternativa a la cuestión del equilibrio entre el control legítimo de los abusos y la protección de los datos personales. Este tipo de identidad se asignaría a una persona a través de un proveedor de servicios especializado. De este modo se respetaría en principio el anonimato, pero el proveedor de servicios especializado podría reconstruir un enlace con la verdadera identidad del titular en determinados casos, tales como la sospecha de que existan actividades delictivas. Respecto al correo electrónico, los reexpedidores anónimos asignan al usuario una dirección anónima a la que otras personas pueden enviar sus mensajes y desde la que éstos se reenviarán a la verdadera dirección del usuario (lo que a veces se denomina servidor seudónimo), o bien envían el mensaje del emisor sin mencionar su nombre ni su dirección[126].

Indización sistemática de los datos

También existen herramientas para garantizar que los autores de páginas personales no estén sujetos a la indización sistemática de sus páginas y a la recopilación de sus datos personales sin tener conocimiento de ello. El objetivo del *protocolo* de exclusión de robots es impedir que un motor de búsqueda pueda indizar automáticamente todas o parte de las páginas de un sitio web[127]. La mayoría de los motores de búsqueda existentes en la Web pueden identificar este *protocolo*. El fichero "robots.txt", incluido en la dirección de Internet, contiene instrucciones para los robots de búsqueda en las que se establece que algunos de ellos no son bienvenidos o que sólo pueden leerse o indizarse algunas páginas identificadas en el sitio.

Dado que sólo un proveedor de servicios puede insertar un *protocolo* de exclusión de robots en la dirección del sitio, los autores de páginas web cuyo proveedor de servicios no acepte incorporar dicho *protocolo* pueden incluir una *metaetiqueta* de robots en cada

[124] En su versión pública de 12 de julio de 2000, COM(2000) 385.

[125] Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, adoptado por el Grupo de Trabajo el 23 de febrero de 1999.

[126] Los responsables del reenvío de primera generación se llaman Cipherpunk, mientras que los de segunda generación, que emplean técnicas más avanzadas, se denominan Mixmaster. Los servidores anónimos más famosos en la red eran "anon.penet.fi" o "alpha.c2.org". Sin embargo, parece que ninguno de los dos sigue operativo hoy en día. Uno nuevo es "Nym.alias.net". Los mensajes anónimos también pueden enviarse a través de un documento HTML. En este caso, el mensaje y el destinatario final se envían sin encriptar al servidor WWW utilizado.

[127] Dictamen 3/99, véase más arriba.

una de las páginas que no quieran que se indice. La desventaja de estas *metaetiquetas* es que no todos los motores de búsqueda existentes en Internet las reconocen.

Acceso en línea a información pública

El último tema tratado en este capítulo se refiere al acceso en línea a información pública, que, no obstante, sigue estando sujeta a las normas de protección de la privacidad.

Las soluciones técnicas aplicadas a estas bases de datos pueden ayudar a limitar el uso ilegal de la información que contienen:

- Los criterios de búsqueda deben definirse de modo que los datos sólo puedan utilizarse de acuerdo con el propósito original. El Grupo de Trabajo insistió en su Recomendación de 13 de julio de 2000 sobre guías inversas en que "el responsable del tratamiento (…) tiene la obligación de aplicar las medidas técnicas y de organización que resulten adecuadas en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse (véase el artículo 17 de la Directiva 95/46/CE). Esto significa, por ejemplo, que la base de datos debería diseñarse de forma que permita impedir posibles usos fraudulentos, tales como la modificación ilícita de los criterios de búsqueda o la posibilidad de copiar toda la base de datos o de acceder a ella con objeto de realizar un tratamiento posterior. Por ejemplo, los criterios de búsqueda deben ser suficientemente precisos para permitir la presentación exclusiva de un número limitado de resultados por página. El resultado debería ser que el fin para el que el abonado ha dado su consentimiento quede también garantizado con medios técnicos"[128].

- La consulta en línea de bases de datos se puede restringir, por ejemplo, limitando el campo o los criterios de consulta. No se debería permitir la recopilación de grandes cantidades de datos mediante una consulta amplia, como las primeras letras de un nombre. Del mismo modo, debería resultar técnicamente imposible solicitar sentencias judiciales basándose, por ejemplo, en el nombre de una persona, o solicitar el nombre de alguien a partir de su número de teléfono.

Con este fin, deberían configurarse y utilizarse herramientas técnicas coherentes con los principios jurídicos descritos en este capítulo.

[128] El Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones había adoptado una recomendación similar sobre guías inversas en su reunión de Hong Kong de 15 de abril de 1998: *Aunque las guías inversas no están prohibidas por la ley, son servicios que requieren un consentimiento expreso y voluntario. Deberían garantizarse, al menos, el derecho de oposición y el derecho de acceso, generalmente reconocidos por las normativas vigentes, nacionales e internacionales, sobre protección de datos personales. En cualquier caso, se ha de garantizar a las personas el derecho a ser informadas por su proveedor de servicios de correo electrónico o de telefonía, en el momento de recabar sus datos o, si ya se han abonado, por medios de información específicos, de la existencia de servicios de búsqueda inversa y (si no se exige el consentimiento explícito) de su derecho a oponerse, de forma totalmente gratuita, a esta búsqueda.* El texto completo de esta recomendación se puede obtener en: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm.

VI. Conclusiones

En teoría, los regímenes jurídicos y los medios técnicos disponibles ofrecen una valiosa protección al titular de los datos en lo que respecta a la disponibilidad pública de algunos de sus datos personales en Internet. "El principio de finalidad, en virtud del cual los datos personales no pueden tratarse con fines incompatibles con los especificados en un principio, tiene una importancia fundamental en cuanto a los datos publicados en determinadas circunstancias".

También deberá prestarse especial atención al principio de limitación del período de almacenamiento de datos personales. Estos datos deberían destruirse al cabo de un tiempo razonable, a fin de impedir la elaboración de perfiles que reúnan, por ejemplo, los mensajes enviados por una persona a un foro de debate a lo largo de varios años.

Esas personas deberían conocer el período previsto de almacenamiento y disponibilidad en línea de dichos datos públicos.

En la actualidad, los problemas residen principalmente en la escasez de información de que disponen tanto los titulares como los responsables del tratamiento de los datos sobre las disposiciones jurídicas que han de observar.

Para mejorar la situación, el objetivo principal consiste en incrementar los esfuerzos por conseguir mayor transparencia en Internet y por armonizar la interpretación de los principios fundamentales relativos al control que el titular de los datos puede tener sobre éstos.

La Directiva 97/66/CE, en su versión revisada de 12 de julio de 2000, ofrece una buena oportunidad para armonizar estas cuestiones.

CAPÍTULO 7: TRANSACCIONES ELECTRÓNICAS EN INTERNET

I. Introducción

El comercio electrónico se puede definir como "cualquier forma de transacción en la que la interacción entre los agentes es electrónica en lugar de basarse en intercambios físicos o en un contacto físico directo"[129]. Esta definición abarca las transacciones relacionadas con la compra de bienes o servicios, así como las utilizadas para mejorar la calidad de los servicios o la prestación de nuevos servicios por parte de entidades privadas y públicas.

Teniendo en cuenta la definición anterior, este capítulo, cuyo principal objetivo es estudiar cuestiones relacionadas con Internet, se centrará en las transacciones que tienen lugar a través de la Red y dejará al margen cualquier otra forma de interacción realizada por redes públicas o privadas.

Se prevé que las transacciones electrónicas tengan una repercusión mundial, ya que el comercio electrónico es global por definición y permite a cualquier empresa (independientemente de su tamaño o su volumen de negocios) ofrecer y vender sus productos en todo el mundo.

Las transacciones electrónicas permiten a las organizaciones ser más eficaces y flexibles, trabajar más estrechamente con sus proveedores y cubrir las necesidades y expectativas de sus clientes de una forma nueva con la que antes ni siquiera soñaban.

Sin embargo, para conseguir estos objetivos se necesita una cantidad enorme de información, lo que podría conducir a la invasión de áreas importantes de la privacidad individual.

II. Agentes

Los principales agentes que participan en las transacciones electrónicas son:

- El usuario, en el contexto de la Directiva 95/46/CE, que es la persona física que quiere comprar un producto o solicita un servicio [130].
- El operador de telecomunicaciones, que no participa especialmente en las transacciones comerciales electrónicas pero desempeña una función esencial en el envío de señales que hacen posible toda forma de transmisión electrónica de datos. La directivas prevén para este agente obligaciones específicas relativas a la seguridad.
- El *proveedor de servicios de Internet* que da acceso a Internet.
- El comerciante electrónico, que es la entidad que ofrece productos o servicios a través de la red.
- La plataforma financiera necesaria en la mayoría de los casos y en la que participan tanto el banco del comerciante como el del consumidor, y una pasarela de pagos que se encarga de los aspectos técnicos necesarios para autorizar la operación financiera y el pago. Esta pasarela de pagos se encarga de todas las conexiones entre instituciones financieras que posibilitan el intercambio de dinero digital asegurando que todos los agentes cumplen los requisitos necesarios para realizar la transacción.

---

[129] Oficina de Proyectos de la Sociedad de la Información de la Comisión Europea, *Electronic Commerce - An Introduction* (http://www.ispo.cec.be/ecommerce/answers/introduction.html).

[130] En la actualidad, la mayoría de las transacciones comerciales electrónicas (en torno al 90 %) se realizan entre empresas (es decir, entre personas jurídicas) que no están cubiertas por la Directiva 95/46/CE (véanse la letra a del artículo 2 y el apartado 1 del artículo 3).

- *Terceros de confianza*, que son necesarios, en los casos más complejos y en que la seguridad es primordial, para autentificar las partes y proporcionar una *encriptación* suficientemente fuerte, con el fin de garantizar la confidencialidad de la transacción.

Existen tres modelos diferentes de transacción electrónica, dependiendo de las formas de comercio y de los agentes u operadores que participen en él[131].

1) Suministro en línea de bienes y productos inmateriales. Utilizado principalmente por casas de desarrollo de software y empresas de comunicaciones en las que la infraestructura de Internet resulta ideal para la venta y distribución remota en tiempo real. Abarcan software, películas de vídeo, juegos y música en línea, así como suscripciones en línea a publicaciones, revistas o programas de apoyo técnico.

En este caso, aparte del ahorro obvio derivado del acceso directo a los consumidores, lo que evita la dependencia de intermediarios, las empresas que utilizan este tipo de comercio tienen una gran ventaja: pueden obtener información precisa y exacta del consumidor final, sus aficiones, intereses y hábitos de compra.

Esta categoría también abarca a la mayoría de los servicios que ofrecen las organizaciones del sector público, como la autoliquidación o devolución tributaria en línea, los formularios electrónicos o las peticiones de pagos por prestaciones sociales y las acciones de seguimiento.

2) Solicitud electrónica de bienes materiales. Esta categoría abarca muchos tipos diferentes de empresas, entre las que se incluyen, en primer lugar, las grandes empresas que utilizan Internet para tener acceso directo al consumidor. Los fabricantes de hardware de tecnología de la información y los minoristas han sido los primeros en usar este canal comercial, lo que es fácilmente comprensible dada la naturaleza del usuario de Internet. En la actualidad, cada vez son más numerosas las empresas que venden ropa, perfumes, libros, CD, billetes de avión, etc.

Internet brinda a las pequeñas y medianas empresas la oportunidad de desarrollar nuevas actividades comerciales a una escala que sería inalcanzable con sus recursos tradicionales. De hecho, y como han advertido algunos observadores, hay una gran diferencia entre la inversión inicial necesaria para ofrecer cien mil CD musicales en una tienda electrónica de Internet y tratar de hacerlo abriendo una tienda en el centro de una ciudad.

Además, todos los sitios de comercio electrónico que suministran bienes materiales dependen en última instancia de una organización logística para entregar los artículos al consumidor final en su dirección personal. Hoy en día, tales organizaciones logísticas están invirtiendo en tecnología de Internet de apoyo a los pedidos electrónicos y la trazabilidad de los envíos entre empresas socias y entre la empresa logística y el consumidor final, de tal forma que todos los participantes pueden averiguar en tiempo real la ubicación de los bienes solicitados y cuándo se espera que se entreguen. En este contexto es bastante posible que determinados distribuidores y expertos en logística decidan fusionarse en un futuro próximo para poder utilizar la información clave que poseen las empresas logísticas acerca del proceso de distribución (principalmente, direcciones de recogida y suministro).

3) Redes y centros comerciales. El comercio en línea no excluye a los distribuidores tradicionales que no tienen un conocimiento particular de las nuevas tecnologías. Éstos tienen la posibilidad de integrarse en una estructura denominada "centros comerciales

[131] La siguiente clasificación se ha tomado de un estudio realizado por la Comisión de las Comunidades Europeas *"On-line services and data protection and the protection of privacy"*, disponible en http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf.

virtuales", que les brinda la oportunidad de combinar sus mercancías en los escaparates de un centro comercial virtual. En estos centros, las tiendas están clasificadas por categorías y los visitantes utilizan un sistema interno de búsqueda para encontrar una lista de sitios que ofrecen el producto solicitado. Se pueden colocar *pancartas* publicitarias basándose en las palabras clave mecanografiadas o en las tiendas visitadas, y el centro comercial virtual ofrece a sus miembros una infraestructura de pago segura.

Dependiendo de su función, es frecuente que los centros comerciales virtuales recojan información muy detallada y exacta sobre sus visitantes y compradores (tiendas visitadas, intereses, hábitos de compra, direcciones, detalles personales e información sobre el pago) que puede resultar de gran interés para establecer perfiles de consumidores a la hora de desarrollar estrategias publicitarias o comerciales[132].

El papel de estos centros comerciales puede cambiar en el futuro si se integran en sitios más amplios, los denominados *portales*, "supersitios" web que proporcionan una gama de servicios entre los que se incluyen la búsqueda en la Web, noticias, guías de páginas blancas y amarillas, mensajería electrónica gratuita, grupos de debate, compras en línea y vínculos con otros sitios.

Estos *portales* modernos ofrecen oportunidades cada vez mayores de realizar compras en todo el mundo, tanto mediante anuncios clasificados como a través de motores de búsqueda. Además, nada impide que en un futuro próximo ofrezcan sus propias plataformas seguras de pago y agentes usuarios inteligentes que puedan buscar en la Web, negociar precios (incluso los términos de privacidad de un contrato comercial)[133] y celebrar acuerdos en nombre del consumidor.

III. Seguridad en los pagos

La creciente importancia del comercio electrónico lleva consigo una necesidad de sistemas de pago adecuados para la venta de bienes y servicios. Dos de los factores que limitan la expansión del comercio electrónico son las preocupaciones acerca de los riesgos que implica el envío por Internet de detalles sobre la tarjeta de crédito y la posibilidad de que se revele información personal confidencial a terceros no autorizados.

Se han desarrollado y se siguen desarrollando diversos métodos para abordar estas preocupaciones. Hoy en día, el más común de ellos es la capa de conexiones seguras[134], que se implementa en los navegadores más utilizados y establece un canal seguro entre los ordenadores del consumidor y del comerciante a través de *encriptación* y *certificados electrónicos*.

El sistema de capa de conexiones seguras funciona, básicamente, como sigue. Antes de que el ordenador del comerciante (servidor) pueda iniciar una conexión segura con el ordenador del consumidor (cliente), el cliente ha de asegurarse de estar conectado a un

---

[132] La forma en que se recoge esta información se explica con más detalle en el capítulo 5, "Navegación y búsqueda".

[133] Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS), adoptado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 16 de junio de 1998. (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm). Véase también el libro de HAGEL III, J. y SINGER, M., *Net Worth: the emerging role of the informediary in the race for customer information*, Harvard Business School Press, 1999 y el informe *Intelligent software agents and privacy*, de J. BORKING, B.M.A. VAN ECK y P. SIEPEL, Registratiekamer en colaboración con el Comisario de información y privacidad de Ontario, Achtergrondstudies y verkenningen, enero de 1999, disponible en www.registratieakamer.nl.

[134] Se puede consultar una descripción completa del sistema de capa de conexiones seguras en http://developer.netscape.com/tech/security/ssl/howitworks.html y http://home.netscape.com/eng/server/console/4.0/help/app_ssl.htm.

servidor seguro. Para comprobar la identidad del servidor se utiliza su *certificado electrónico*. Una vez que se ha autentificado el servidor, el cliente y éste pueden encriptar los datos que se envían y garantizar su *integridad*, incluido el número de tarjeta de crédito que se use en la transacción y cualquier otro detalle personal.

Conviene tener en cuenta que el sistema de capa de conexiones seguras no permite al consumidor controlar el uso o tratamiento que el comerciante haga posteriormente de sus datos personales, y que la *autentificación* del cliente no es obligatoria, con lo que el uso indebido de la identidad de otra persona constituye una posibilidad de fraude.

Para tratar estas dificultades y proporcionar un marco totalmente fiable en las transacciones comerciales electrónicas, algunas empresas de tarjetas de crédito han desarrollado conjuntamente un nuevo *protocolo* con el apoyo de los principales desarrolladores de software. Este *protocolo*, denominado SET ("*secure electronic transactions*" o transacciones electrónicas seguras), proporciona transmisiones confidenciales (utilizando la *encriptación*), *autentificación* de las partes (titular de la tarjeta, emisor, vendedor, comprador y pasarela de pagos a través de certificados electrónicos), e *integridad* e irrevocabilidad de los pagos de bienes y servicios (mediante *firmas electrónicas*)[135].

Dado que el sistema mencionado no es muy adecuado si se necesita realizar un número elevado de transacciones de pequeño valor, se está desarrollando un método alternativo denominado dinero digital o "*e-cash*". El principio general consiste en descargar el dinero en el disco duro de un ordenador (o, en un futuro próximo, en el chip de una tarjeta inteligente). Cada vez que se efectúe un pago en línea, el usuario transferirá unidades de dinero (fichas) desde su ordenador o tarjeta inteligente a la cuenta del vendedor o del proveedor de servicios. En esta área hay varias tecnologías en competición. Las más interesantes desde el punto de vista de la protección de la información personal son los sistemas de pago completamente anónimo basados en un mecanismo de firma ciega[136]. Estos mecanismos podrían impedir la trazabilidad de las transacciones, pues el banco que "firma" el *e-cash* no vincula al consumidor con una transacción concreta.

IV. Riesgos para la privacidad

Independientemente del tipo de transacción realizada o del sistema de pago utilizado, la diferencia esencial entre el mundo físico y el electrónico es que muchas actividades del primero pueden quedar en el anonimato (mirar escaparates, pasear por diversas tiendas, examinar productos y, si se paga en efectivo, comprar bienes), mientras que en el

[135] Utilizando el *protocolo* SET durante la transacción, las partes se comunican por medio de dos pares de claves de *encriptación* únicas y asimétricas: claves de *encriptación* públicas para firmar documentos relativos a la transacción (es decir, la oferta de compra) y claves privadas, entre las que se incluye la *firma electrónica* de la transacción real (es decir, la instrucción de pago), que garantizan la *integridad* de la transmisión y que la orden no sea revocada. El sistema funciona como una doble firma: ambas claves interactúan de tal forma que un pago no se puede validar a menos que la oferta de compra sea aceptada por el vendedor y la orden real no se paga hasta que la institución financiera ha dado su aprobación. El vendedor no conoce las instrucciones de pago y el banco no tiene acceso a los contenidos de la orden. Para obtener una descripción funcional del complejo *protocolo* SET, *véase SET Secure Electronic Transaction Specification Book 1*. En http://www.setco.org/download.html se puede consultar una descripción comercial. Véase también GARFINKEL, S., *Web security and commerce*, Oreilly associates, junio de 1997, capítulo 12: *Understanding SSL and TLS.*

[136] Para acceder a un debate teórico sobre cómo funcionan estos sistemas, véase, CHAUM, David *"A Cryptographic Invention Known as a Blind Signature Permits Numbers to Serve as Electronic Cash or to Replace Conventional Identification. The Author Hopes It May Return Control of Personal Information to the Individual"* http://www.eff.org/pub/Privacy/chaum_privacy_id_Article, que se publicó en *Scientific American* en agosto de 1992.

segundo puede grabarse todo, añadirse a información previa o nueva y tratarse casi sin ningún coste para producir información más amplia sobre cada persona. Y todo ello puede hacerse sin el consentimiento del ciudadano afectado e incluso sin su conocimiento. Además, con las actuales tecnologías de *almacenamiento de información* y *minería de datos*[137] se puede tratar una cantidad enorme de información, no sólo para seleccionar a las personas que cumplen ciertos requisitos o criterios, sino también para descubrir relaciones ocultas entre datos sin una conexión aparente, con lo que se explicitan algunos patrones de conducta que se podrían utilizar para tomar decisiones comerciales o administrativas en relación con determinados ciudadanos.

En la mayoría de los casos, cuando un sujeto registrado realiza una compra o contrata un servicio (como una suscripción), es obligatorio que proporcione detalles personales al vendedor o al proveedor de servicios para que lo autentifique, se garantice el pago y se comunique una dirección física o electrónica para la entrega de los bienes o servicios. De este modo, a menos que se pague utilizando *e-cash* o tecnologías de protección de la privacidad para ocultar la dirección IP y comprar un bien inmaterial, hoy en día es muy raro que el anonimato sea posible en la red.

Este capítulo se centrará en los riesgos asociados al uso secundario no autorizado de datos personales y en los relacionados con el incumplimiento de la confidencialidad o la suplantación de la personalidad.

1. Uno de los usos secundarios de datos personales más frecuentes es la publicidad. Una vez identificado el comprador, bien porque sea él mismo quien proporcione información al conectarse al servidor, bien a través de otros dispositivos tecnológicos como las *cookies*, se utiliza información previa sobre él para hacer publicidad personalizada según sus hábitos, intereses, *series de clics* o hábitos de compra. Y no se trata sólo de anuncios relacionados con los servicios y las ofertas del propietario del sitio web, sino también de los emitidos por terceras partes que tienen acuerdos para apoyar el coste derivado de la gestión del servidor mediante la exposición de sus anuncios publicitarios.

Los paradigmas de la publicidad de Internet son las técnicas utilizadas por agencias publicitarias como DoubleClick, cuyas actividades se basan en proporcionar espacio publicitario en la Red y facilitar a los anunciantes la elección del espacio adecuado para sus actividades de comunicación. El otro elemento vital en el éxito de DoubleClick es la tecnología de la información, que hace posible aislar criterios de identificación y ofrecer a los anunciantes herramientas para dirigir a los usuarios anuncios individualizados. Esta tecnología recurre a una base de datos que contiene información acerca de varios millones de usuarios de Internet, con lo que se garantiza que durante las campañas publicitarias sólo se contactará con la audiencia deseada.

Para lograrlo, DoubleClick recoge y trata datos personales que permiten identificar a los usuarios, describir sus hábitos y determinar en tiempo real los elementos de la población que probablemente satisfarán los criterios de los objetivos de las campañas publicitarias existentes. DoubleClick asigna un número de identificación único a cada usuario que visita uno de los sitios web de su red y coloca una *cookie* que más tarde se utilizará para identificar al usuario cuando se conecte a otro de los sitios de DoubleClick y, de acuerdo con los datos que se tengan de tal usuario, personalizar el anuncio más adecuado. Aunque el visitante no acepte la *cookie* se puede elaborar su perfil, sobre todo si tiene una dirección IP estática.

[137] Véase el informe de la Registratiekamer (BORKING, J., ARTZ, M. y VAN ALMELO, L.), *Gouden bergen van gegevens: over datawarehousing, datamining en privacy*, Achtergrondstudies en verkenningen, 10 de septiembre de 1998, disponible en www.registratiekamer.nl.

Los datos personales registrados en la base de datos de DoubleClick son los siguientes: parte permanente de la dirección IP (es decir, la dirección en la Red), dominio, país, Estado (en Estados Unidos), código postal, código SIC (código del Sistema de clasificación industrial normalizada, EE.UU.), tamaño y volumen de negocios de la empresa (optativo), sistema operativo utilizado y número de versión del mismo, proveedor del servicio, número de identificación (asignado por DoubleClick) y referencia de las actividades de navegación (recogida y análisis de sitios visitados por el usuario)[138].

El 23 de noviembre de 1999 DoubleClick se fusionó con Abacus Direct Corporation. Abacus, que ahora es un departamento de DoubleClick, seguirá explotando Abacus Direct, el elemento de publicidad directa de Abacus Alliance. Además, se ha anunciado que Abacus ha empezado a crear Abacus Online, el elemento de Internet de Abacus Alliance.
De acuerdo con la información disponible en el sitio web de DoubleClick, la parte de Abacus Online de Abacus Alliance permitirá a los usuarios estadounidenses de Internet recibir mensajes publicitarios personalizados según sus intereses individuales[139].
Una ciudadana californiana presentó una demanda relativa a dicha fusión ante el Tribunal Supremo del Estado de California tratando de conseguir un requerimiento judicial contra DoubleClick por realizar en Internet prácticas comerciales fraudulentas y engañosas que violan los derechos de privacidad del público en general. La demanda también afirmaba que DoubleClick engaña y ha engañado al público en general *"(...) dándole una idea falsa de la privacidad y de la seguridad en su uso de Internet, adquiriendo, almacenando y vendiendo, de un modo encubierto, millones de datos privados e íntimos de los usuarios de Internet, y sacando provecho de ello. (...) Cuando un usuario de Internet visita un sitio web participativo, una* cookie *con una identificación única se coloca en su ordenador. A partir de ese momento, cada vez que ese usuario visite un sitio web que contenga información sobre su identidad (...), ésta se vinculará a la* cookie *identificativa. Los demandados son capaces de obtener una cantidad potencialmente grande de información personal sobre el usuario utilizando la base de datos Abacus. Por otra parte, los hábitos de compra del usuario de Internet, sus respuestas a la publicidad y los sitios web que visita se rastrean y registran"*[140].

DoubleClick afirma que, dadas las reacciones públicas ante este proyecto de cotejar su base de datos con la de Abacus, hasta ahora no se han dado los pasos efectivos para lanzar tal unión.

Otro ejemplo de cómo tratar los datos personales de una forma que el usuario medio de Internet no puede esperar es el trabajo que realiza SurfAid, una pequeña empresa que forma parte del departamento de servicios globales de IBM situado en Somers (Nueva York)[141]. Esta empresa recibe a diario los ficheros históricos de acceso de sus clientes y los pretrata para averiguar la ruta que han seguido los visitantes del sitio web cliente. A continuación se utilizan diversas herramientas de *minería de datos* de gran capacidad para explorar el archivo del cliente, que en algunos casos contiene más de ciento cincuenta millones de peticiones de información, y se produce un informe diario al que pueden acceder los clientes. Posteriormente, el cliente puede utilizar programas de *OLAP* para desglosar y analizar la información.

---

[138] Como se menciona en el estudio *On-line services and data protection and privacy*, de GAUTHRONET, S. y NATHAN, F., publicado por la Comisión de las Comunidades Europeas y disponible en http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/serven.pdf.
[139] www.doubleclick.net:8080/privacy_policy/.
[140] Harriet M. Judnick contra DoubleClick, Inc.
[141] WATTERSON, Karen, *La minería de datos ya es una tendencia dominante*; DATAMATION (Edición española), febrero de 2000.

2. Otro riesgo al que se enfrentan las personas cuando realizan transacciones comerciales es el incumplimiento de la confidencialidad de la información transmitida. Dado que Internet es una red pública abierta con *protocolos* bien conocidos y destinados a compartir información más que a proteger la confidencialidad o seguridad, no resulta muy difícil, para quienes tengan algunos conocimientos técnicos, encontrar numerosas herramientas de programación que permitan interceptar y revelar los datos transmitidos a través de la Red. También es posible hacerse pasar por una empresa o institución para obtener información que, posteriormente, se podría utilizar para cometer algún fraude o delito.

3. Se está desarrollando una nueva forma de comercio: el comercio electrónico móvil, basado en la tercera generación de teléfonos celulares y otros aparatos portátiles que pueden acceder de forma segura al comercio electrónico y a las páginas web gracias a la utilización de un nuevo *protocolo*[142]. Por consiguiente, la localización y el tráfico de datos, así como los hábitos de viaje, se pueden añadir a los datos sobre transacciones y navegación para elaborar un perfil incluso más detallado del consumidor. Y si se tienen en cuenta las fusiones y las concentraciones entre empresas de telecomunicaciones, proveedores de servicios, *portales* y empresas de contenido, la posibilidad de agregación, integración y tratamiento conjunto aumenta de manera exponencial.

A modo de simple ejemplo de lo que podría ocurrir en un futuro próximo, se puede prever que los anuncios publicitarios perseguirán por todas partes a las personas a través de sus teléfonos móviles o sus asistentes electrónicos personales. "Es un tipo de posicionamiento global de los objetivos, y no está lejos" afirmó un portavoz de DoubleClick[143].
Otro ejemplo es el proyecto conjunto de Yahoo! y CellPoint Systems AB para comercializar un localizador personal utilizando teléfonos móviles. El sistema "Find-A-Friend" de Yahoo! se puede utilizar para obtener información del tipo: "Juan está cerca de Piccadilly Circus, más o menos a 3,2 km de tí en dirección noroeste", gracias a los recursos de la red GSM de teléfonos móviles. Aunque se exige el consentimiento personal para entrar a formar parte del plan, este ejemplo nos muestra las posibilidades de las nuevas tecnologías de las telecomunicaciones, que pueden localizar al usuario mediante aparatos portátiles[144].

V. Análisis jurídico

Antes de nada conviene recordar que, como ya se explicó detalladamente en el capítulo 3, las normas sobre protección de datos de las Directivas 95/46/CE y 97/66/CE son aplicables a Internet y a los datos personales tratados en las transacciones electrónicas[145]. Los párrafos que siguen se centrarán en los aspectos de estos textos legales especialmente pertinentes en el ámbito de las transacciones electrónicas.

Legitimidad del tratamiento: principio de finalidad (artículos 5 a 7 de la Directiva 95/46/CE)

El primer aspecto que cabe considerar es que tanto la recogida de datos como su tratamiento se haga de forma justa y legal, teniendo en cuenta los principios de finalidad y proporcionalidad. En el contexto de las transacciones electrónicas, es importante

[142] *Protocolo* de aplicación inalámbrica (*WAP*).
[143] Jane Weaver, MS NBC, 16/04/2000.
[144] Para más información, véase http://www.cellpt.com/v2/000504.htm.
[145] Tratamiento de datos personales en Internet, documento de trabajo aprobado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 23 de febrero de 1999 (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm).

considerar que la recogida de datos personales puede resultar "invisible" para su titular. El Grupo de Trabajo ha comunicado con frecuencia su preocupación acerca de todos los tipos de operaciones de tratamiento que en la actualidad se realizan en Internet mediante software y hardware sin el conocimiento del interesado, y que, por lo tanto, resultan "invisibles" para él[146].
Cuando se recaban datos personales sobre un usuario de Internet, se le debe dar información clara acerca del propósito de su tratamiento y de los destinatarios y categorías de destinatarios de tal información, de manera que el interesado pueda decidir si desea llevar a cabo la transacción en dichas condiciones.

Por otra parte, también se habrían de explicitar los usos secundarios de datos personales, que, en caso de que no se consideren compatibles con el propósito principal, deberían estar sujetos al consentimiento del interesado. Algunos ejemplos de usos secundarios incompatibles son la comunicación de datos sobre transacciones a terceras partes para permitirles establecer perfiles de compradores en sus campañas publicitarias[147] o la utilización de herramientas de *minería de datos* para averiguar los hábitos de comportamiento de una lista de nombres de sitios web visitados por un usuario de Internet.

Conviene destacar que el consentimiento del usuario registrado, necesario para tratar sus datos personales en el marco de una transacción comercial electrónica, no es preciso para recabar los datos que se necesitan para realizar tal transacción. En sí mismo, esto constituye una base legítima para procesar los datos personales del usuario necesarios en esta tarea, como se afirma en la letra b) del artículo 7 de la Directiva. Cualquier otro dato relacionado, incluidos los datos invisibles que no son necesarios para realizar la transacción, sólo se puede tratar partiendo de otras bases legítimas mencionadas en el artículo 7 de la Directiva, es decir, consentimiento inequívoco, cumplimiento de las obligaciones jurídicas, interés vital del interesado o interés legítimo de los responsables del tratamiento, siempre que no prevalezcan los derechos fundamentales del interesado. Esto también es aplicable a las transacciones de los organismos oficiales, pues la legitimidad de la recogida de datos y el tratamiento de datos personales por parte de los organismos públicos se basa en reglamentaciones jurídicas[148].

Un uso secundario que los responsables del tratamiento de los sitios web personales mencionan a menudo es el mantenimiento técnico y el dimensionamiento del equipo de tecnología de la información. No cabe duda de que se trata de una preocupación legítima si se quiere ofrecer un buen servicio a los clientes, pero que se puede satisfacer plenamente utilizando datos no identificables, pues para dimensionar los ordenadores y las líneas de telecomunicaciones basta con cifras agregadas. Los responsables de tratamiento sólo pueden conservar datos personales por razones técnicas cuando resulta estrictamente necesario para alcanzar este propósito y es aplicable una de las bases legítimas para el tratamiento de datos.

Información al interesado (artículo 10 de la Directiva 95/46/CE)

Además, el responsable del tratamiento debe proporcionar información precisa al interesado, incluida la identidad del responsable, los fines del tratamiento, los destinatarios de la información, el carácter obligatorio o no de la respuesta y las

[146] Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por *software* y *hardware*, adoptado por el Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales el 23 de febrero de 1999 (http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm).
[147] Letra b) del artículo 14 de la Directiva 95/46/CE.
[148] Véase también el capítulo 6 en relación con el debate sobre el propósito del principio de especificación aplicado a datos disponibles públicamente.

consecuencias que para él tendría una negativa a responder y la existencia de derechos de acceso y rectificación de los datos que le conciernen. Si existe la posibilidad de que el titular se oponga al tratamiento, también se le ha de informar de ello.

El interesado debería recibir información directamente en la pantalla en la que se recaba la información o mediante un cuadro de diálogo, tal como se explica en el capítulo 5.

En los sitios web resulta muy fácil proporcionar al interesado la información y comprobar que dispone como mínimo de la oportunidad de leerla mostrándosela como una parte obligatoria del proceso de la transacción, antes de que tome ninguna decisión. Para garantizar con toda certeza que las cláusulas mostradas no se modifican posteriormente, pueden incluir una *firma electrónica* de las cláusulas creadas con la clave privada del vendedor. De esa forma, el usuario cuenta con una prueba de las condiciones con las que se ha declarado de acuerdo. Esta idea parece conforme al párrafo 3 del artículo 10 de la Directiva sobre comercio electrónico, que indica que *las condiciones generales de los contratos facilitadas al destinatario deben estar disponibles de tal manera que éste pueda almacenarlas y reproducirlas*[149].

Protección de datos personales/sobre tráfico (artículo 6 de la Directiva 95/46/CE y artículo 6 de la Directiva 97/66/CE)

La letra e) del apartado 1 del artículo 6 de la Directiva expresa la obligación de no mantener datos identificables durante un período superior al necesario para los fines para los que fueron recogidos.

En cuanto al tráfico de datos, se han de respetar las estrictas limitaciones impuestas en el artículo 6 de la Directiva 97/66/CE: el tráfico de datos tendrá que destruirse o hacerse anónimo en cuanto termine la comunicación (en el caso que nos ocupa, la transacción económica).

En su Recomendación 3/99[150], el Grupo de Trabajo abordó la cuestión concreta de la protección de los datos sobre tráfico por parte de los *proveedores de servicios de Internet* con fines de aplicación de la ley. Esta Recomendación subraya que, en principio, los datos sobre tráfico no deberían conservarse a efectos exclusivos de control, y que las legislaciones nacionales no deberían obligar a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y *proveedores de servicios de Internet* a conservar los datos sobre tráfico durante un plazo superior al necesario a efectos de facturación[151].

Decisiones individuales automatizadas (artículo 15 de la Directiva 95/46/CE)

Como ya se ha mencionado anteriormente, los datos relativos a las transacciones no se pueden mantener indefinidamente, sobre todo si se pretende utilizarlos en decisiones automatizadas referentes a personas (como rechazar una petición o denegar que se complete una compra) basadas en datos almacenados previamente.

En este caso, el interesado habrá de recibir las garantías adecuadas[152], que incluyen el derecho de toda persona a no ser objeto de una decisión que le afecte de forma significativa y se base únicamente en el tratamiento automatizado de datos, a menos que

[149] Directiva 2000/31/CE de 8 de junio de 2000.
[150] Véase http://europa.eu.int/comm/dg15/en/media/dataprot/wpdocs/index.htm.
[151] Respecto a este tema, véase también la declaración oficial, ya mencionada, que los Comisarios europeos de protección de datos formularon en Estocolmo, según la cual en los casos específicos en que se han de conservar datos sobre tráfico deberá existir una necesidad demostrable, el período de conservación deberá ser lo más breve posible y la práctica deberá estar claramente regulada por la ley.
[152] Véase también el tercer párrafo de la letra a) del artículo 12 de la Directiva 95/46/CE.

se haya acordado por contrato o así lo autorice una ley, y el derecho a conocer la lógica de cualquier tratamiento automático de datos que afecte al titular.

Derechos de los interesados (artículo 12 de la Directiva 95/46/CE)

También es obligatorio establecer procedimientos claros y eficaces que permitan a los titulares de los datos ejercer sus derechos de acceso, rectificación, supresión o bloqueo. Cuando los titulares ejercen sus derechos, el responsable del tratamiento debe proporcionarles información transparente sobre si sus archivos contienen (o no) datos personales registrados y, en caso de que así sea, sobre qué datos se están tratando, su origen, los fines del tratamiento, las categorías de datos afectadas y los destinatarios o categorías de destinatarios a los que se prevé que se les comunicarán. Esta información debería estar disponible de forma inteligible. Además, en el contexto de las transacciones electrónicas es recomendable que la información se proporcione mediante la conexión en línea establecida, siempre y cuando el interesado no haya solicitado recibirla de otra forma normalizada.

Una cuestión muy importante relativa al acceso a los datos relacionados con transacciones electrónicas o recabados mediante ellas es el derecho de su titular a obtener información no sólo sobre la información básica o primaria, sino también sobre la derivada o consolidada. Esto significa que si se ha elaborado algún tipo de perfil personal, se ha realizado alguna clasificación o división en categorías o se han añadido datos procedentes de terceras partes, esta información tratada también debería estar a disposición del interesado, tal y cómo se especifica en la letra a) del artículo 12 de la Directiva.

Obligaciones del responsable del tratamiento: confidencialidad y seguridad (artículos 16 y 17 de la Directiva 95/46/CE y 4 y 5 de la Directiva 97/66/CE)

Respecto a las cuestiones relacionadas con la confidencialidad y la seguridad, los responsables del tratamiento han de tomar medidas apropiadas para proteger la información que les suministran sus clientes de la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, como ocurre en el caso de las transacciones electrónicas en Internet. Estas medidas han de tener en cuenta los riesgos de seguridad y confidencialidad, la naturaleza de los datos y las tecnologías de vanguardia.

Legislación aplicable (artículo 4 de la Directiva 95/46/CE)

Otra cuestión preocupante en relación con el comercio electrónico en Internet es la legislación aplicable al tratamiento de datos personales recabados de sitios web que están fuera de la UE/EEE. Esto suscita una serie de asuntos problemáticos que deberían analizarse uno a uno. Sin embargo, tal análisis debería tener en cuenta que la Directiva 95/46/CE es claramente aplicable a las operaciones de tratamiento de datos realizadas con equipos localizados, total o parcialmente, en el territorio de la UE, incluso cuando los responsables del tratamiento se encuentran fuera de la Comunidad[153].

VI. Conclusiones

- Al titular de los datos se le debería proporcionar información clara y comprensible que satisfaga plenamente el principio de información. En particular, durante el proceso de transacción electrónica se debería mostrar obligatoriamente la información sobre protección de datos estrechamente relacionada con la realización

[153] Para más detalles, véase el capítulo 3.

de la transacción, con el fin de garantizar que el interesado pueda disponer de ella. Esto ha de entenderse independientemente de la información destinada a los visitantes de sitios web que no realicen compras. Como medida suplementaria, se deberá poner a disposición del interesado una *firma electrónica* de las condiciones de tratamiento de los datos personales para que posteriormente pueda comprobar que tales condiciones no han sido modificadas.

- Se ha de respetar plenamente el principio de proporcionalidad. Sólo se deberán recabar los datos necesarios para la transacción electrónica. Por otra parte, el tratamiento de datos (especialmente si se tratan de una forma que resulta invisible para el interesado) se ha de justificar a partir de una de las bases legítimas mencionadas en el artículo 7 de la Directiva.
- Si el interesado decide no proporcionar más detalles personales que los necesarios para que se realice la transacción electrónica, no se deberá ejercer ningún tipo de discriminación contra él en las condiciones ofrecidas para la transacción.
- No se debe efectuar ningún tratamiento secundario sin el conocimiento del titular de los datos, quien, por otra parte, cuando desee acceder a estos procesos deberá recibir información completa sobre la lógica que los rige. Además, para que el tratamiento se considere legal será necesario un consentimiento sin ambigüedades o alguno de los otros criterios de legitimidad previstos en la Directiva 95/46/CE.
- En la medida de lo posible, se debería utilizar la tecnología de la *encriptación*, sujeta a las reglamentaciones legales existentes, para proteger la confidencialidad de las transacciones electrónicas y garantizar la *integridad* de los mensajes por medio de una *firma electrónica*.
- Cuando sea necesario para dar mayor seguridad a las transacciones, sería recomendable utilizar la tecnología de los *certificados electrónicos*. Si es necesaria una mayor seguridad, estos *certificados* se podrían almacenar en tarjetas inteligentes.
- Desde el punto de vista de la protección de los datos personales, la posibilidad de usar métodos de pago seguros y anónimos es un elemento muy importante de la privacidad en Internet.
- La recogida y el tratamiento de datos personales utilizando equipos automatizados u otros situados en el territorio de la UE/EEE están sujetos a las disposiciones legislativas comunitarias de protección de datos.
- Con relación al tráfico de datos, se han de observar las estrictas limitaciones impuestas por el artículo 6 de la Directiva 97/66/CE y se debería tener en cuenta la Recomendación 3/99 sobre la conservación de los datos sobre tráfico por los proveedores de servicio Internet a efectos de cumplimiento de la legislación.

CAPÍTULO 8: CIBERMARKETING

I. Introducción

Internet no es simplemente una plataforma mundial de información, sino también un mercado mundial en el que empresas competidoras tratan de atraer a clientes potenciales. El éxito depende de llegar a tantos clientes como sea posible, y especialmente a los que de verdad están interesados por el producto o servicio que se les ofrece. Para lograrlo se utilizan perfiles y anuncios publicitarios dirigidos basados en perfiles que se lanzan en *pancartas* colocadas en los sitios web.

Otra forma de conseguir clientes, considerada a veces la más eficaz, es el correo electrónico comercial y el envío de un gran número de mensajes no solicitados a direcciones de personas encontradas en espacios públicos de Internet. Este impopular tipo de correo electrónico se denomina *buzonfia* ("spam")[154].

En ambos casos es necesario poseer datos personales de los clientes, que a menudo se pueden recabar fácilmente en Internet. Muchos usuarios de Internet no son conscientes de que mientras están navegando por la red dejan tras ellos un gran volumen de datos que se pueden utilizar para hacer suposiciones sobre sus intereses, sus preferencias y su comportamiento[155].

La publicidad dirigida puede ser aceptable hasta cierto punto, cuando va en interés del consumidor; pero si el usuario no sabe qué datos se están recabando, quién los recopila ni con qué fin serán utilizados, pierde el control de sus datos personales. Por lo tanto, no es correcto recabar datos sin el consentimiento y el conocimiento del usuario.

II. Descripción técnica

Publicidad y elaboración del perfil en línea[156]

La elaboración del perfil personal en línea se puede realizar de diferentes formas:

- Un sitio web crea perfiles mediante la recogida de datos sobre sus clientes que se basan en las interacciones con ellos. Para hacerlo se utilizan *cookies* que rastrean las acciones del usuario en la Web. Dependiendo de cómo esté configurado el navegador del usuario, éste puede no ser consciente de que el sitio web está instalando una *cookie* en su ordenador. Basándose en el perfil del cliente, el sitio web le ofrecerá productos (por ejemplo, libros) o referencias a otros sitios web que le pueden interesar.
- En el ámbito del "cibermarketing de incentivos", los usuarios pueden participar en un juego o un concurso siempre y cuando proporcionen datos personales que servirán para elaborar los perfiles. En este caso, normalmente el titular de los datos está al corriente de que se han recabado, y por lo tanto da su consentimiento[157].

---

[154] Véase el apartado V, "Análisis de cuestiones especiales. Buzonfia", del capítulo 4, "Correo electrónico".

[155] Véanse, en el capítulo 5, "Navegación y búsqueda", más detalles sobre los datos generados durante el proceso de navegación.

[156] En este contexto es importante mencionar la posición común referente a los perfiles en línea de Internet, adoptada por el Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones en la 27ª reunión del Grupo de Trabajo, celebrada los días 4 y 5 de mayo del 2000 en Rethymnon / Creta. El texto de esta recomendación está disponible en: http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm.

[157] Sólo será así cuando un sitio web ofrezca información suficiente al usuario sobre los datos tratados, el fin del tratamiento, la identidad del responsable del tratamiento, etc. Véase el artículo 10 de la Directiva.

- Empresas publicitarias de la Red (como DoubleClick o Engage[158]) gestionan y proporcionan *pancartas* publicitarias[159] (en lo sucesivo, *pancartas*) sobre una base contractual en muchos sitios web. Las *pancartas* se colocan en el sitio web solicitado mediante un *hipervínculo* invisible con la empresa de publicidad.
  Para hacer llegar al cliente la *pancarta* más adecuada, los anunciantes de la red elaboran perfiles mediante *cookies* colocadas a través del *hipervínculo* invisible. Dependiendo de la configuración del navegador, el usuario puede ser consciente de que se está colocando una *cookie* y tiene la opción de dar o no dar su consentimiento. El perfil del cliente está vinculado al número de identificación de la *cookie* de la empresa publicitaria, de modo que se puede ampliar cada vez que el cliente visita un sitio web que ha firmado un contrato con el anunciante.

Tras ser analizados, los datos recabados se pueden completar con información demográfica (edad, género, etc.) y combinarse con otros datos característicos del grupo al que es obvio que pertenece el usuario, determinado por su comportamiento en la red (por ejemplo, por sus intereses). El trabajo de analizar y completar los datos lo pueden realizar programas especiales (especialmente herramientas de *minería de datos*) disponibles en el mercado.
Estos procedimientos dan como resultado perfiles muy detallados que permiten a la empresa o al anunciante de la Red prever los gustos, las necesidades y los hábitos de compra del consumidor y, a partir de estas premisas, hacerle llegar *pancartas* que se adecuen lo más posible a sus intereses.
Cuando los datos recabados, reunidos mediante el número de identificación de la *cookie* del anunciante, no están vinculados a datos identificables[160] de una persona en concreto, se pueden considerar anónimos. Pero en circunstancias frecuentes, por ejemplo cuando el cliente rellena un pedido en el sitio web en que el anunciante ha colocado la *pancarta*, los datos identificables se podrían vincular o unir a datos existentes ya situados en la *cookie*, lo que permitiría elaborar un perfil identificable de la persona en cuestión[161].

Correo electrónico comercial

Para realizar una campaña comercial por correo, una empresa tiene que conseguir una lista extensa y apropiada de direcciones de correo electrónico de usuarios potenciales. Como ya se ha mencionado, a menudo resulta muy fácil utilizar recursos disponibles en Internet.
Existen tres formas diferentes de recabar direcciones de correo electrónico a partir de Internet[162]: recogida directa de clientes o visitantes de sitios web, compra o alquiler de

[158] Se pueden encontrar más detalles sobre las técnicas utilizadas por tales empresas publicitarias en el apartado "Riesgos para la privacidad" del capítulo 5, "Navegación y búsqueda", así como en el capítulo 7, "Transacciones electrónicas en Internet".
[159] Las *pancartas* publicitarias son pequeños cuadros gráficos que aparecen sobre el contenido de un sitio web o integrados en él.
[160] Conviene tener en cuenta que la definición de datos identificables de la letra a) del artículo 2 de la Directiva CE/95/46 es muy amplia: "se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".
[161] Véase el apartado I, "Cuestiones jurídicas generales: Datos personales en Internet", del capítulo 3, "Aplicación de la legislación relativa a la protección de datos".
[162] Se pueden obtener más detalles sobre la recogida de direcciones de correo electrónico en el capítulo 4, relativo al correo electrónico.

listas a terceros[163] y recogida a partir de espacios públicos[164] tales como guías públicas de correo electrónico o listas de correo electrónico, foros de debate o salas de charla.
Ciertas herramientas disponibles en Internet ayudan a recabar direcciones de correo electrónico. Estos programas buscan sitios web o partes de la Usenet que se han de especificar de antemano mediante una lista de URL o de palabras clave relacionadas con un ámbito de interés predefinido (por ejemplo, deporte, viajes, etc.) y posteriormente proporcionan todas las direcciones de correo electrónico que se han encontrado en los sitios/páginas o en los foros. Existen diversos servicios que funcionan como corredores de listas, recabando direcciones de correo electrónico y vendiéndolas o alquilándolas a precios muy bajos.
Además, hay otras herramientas especializadas en enviar mensajes como "proveedores de servicios de correo electrónico", es decir, sin utilizar un *proveedor de servicios de Internet* ni ningún otro proveedor que ofrezca un servicio de correo electrónico. Por una parte, estos programas garantizan que se esquivan todos los filtros antibuzonfia instalados por dichos proveedores, y por otra permiten un funcionamiento rápido y automático. Si el emisor lo desea, puede recurrir a un servidor de *buzonfia*, en el que un tercero se encarga de este tipo de envíos, también a bajo precio.

III. Análisis jurídico

Existen diversas directivas aplicables a la elaboración de perfiles en línea y al correo electrónico comercial.

La Directiva de protección de datos

La Directiva general establece que los datos personales se traten de manera leal, se recojan con fines determinados, explícitos y legítimos y se utilicen de forma leal y legal de acuerdo con los fines establecidos[165].
El tratamiento debe desarrollarse sobre bases legítimas como el consentimiento, un contrato, la ley o el equilibrio de intereses[166]. Por otra parte, se ha de informar al interesado del tratamiento que se quiera realizar, lo que incluye la comunicación a terceros, antes de que ésta tenga lugar[167], y el titular tiene derecho a oponerse al tratamiento de sus datos personales con fines comerciales directos[168]. El interesado también tiene derecho a acceder a sus datos, rectificarlos, suprimirlos o bloquearlos[169].

La Directiva de venta a distancia

La Directiva de venta a distancia[170] establece, como mínimo, el derecho de los consumidores a oponerse a las comunicaciones a distancia realizadas por medio de correo electrónico[171].

---

[163] Estas listas también pueden contener direcciones de correo electrónico recogidas de espacios públicos de Internet.
[164] Véase el capítulo 6 acerca de publicaciones y foros.
[165] Artículo 6 de la Directiva 95/46/CE.
[166] Artículo 7 de la Directiva 95/46/CE.
[167] Artículo 10 de la Directiva 95/46/CE.
[168] Artículo 14 de la Directiva 95/46/CE.
[169] Artículo 12 de la Directiva 95/46/CE.
[170] Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia.
[171] Artículo 10 de la Directiva 97/7/CE.

La Directiva específica sobre la intimidad en las telecomunicaciones

La Directiva 97/66/CE da a los legisladores nacionales la posibilidad de aplicar normas que les permiten optar por recibir o no recibir comunicaciones comerciales que no hayan solicitado[172]. Los casos en los que se utilicen aparatos de llamada automática o faxes con fines de venta directa están sujetos al consentimiento previo del consumidor[173]. La definición de aparatos de llamada automática, formulada en términos muy imprecisos, se podría aplicar fácilmente al correo electrónico.

En julio de 2000, la Comisión Europea presentó una propuesta de Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas en sustitución de la Directiva 97/66/CE.
En esta propuesta, el artículo relativo a las comunicaciones comerciales no solicitadas incluye de manera explícita el correo electrónico, que sólo está permitido en caso de que los abonados hayan dado su consentimiento previo.

La Directiva de comercio electrónico

La Directiva de comercio electrónico[174] establece que los mensajes electrónicos comerciales han identificarse como tales[175] y que los registros de no participación, en los que pueden inscribirse las personas que no deseen recibir tales mensajes electrónicos, se deben consultar periódicamente y se han de respetar[176].
Aunque ni la Directiva general ni la de telecomunicaciones se refieren explícitamente al comercio electrónico, se deben aplicar a este ámbito: los considerandos y la letra b) del apartado 5 del artículo 1 de la Directiva sobre comercio electrónico establecen claramente que dicha Directiva no está en modo alguno destinada a modificar los principios y requisitos legales del marco legislativo existente. De ello se deduce que la ejecución de la Directiva sobre comercio electrónico ha de estar totalmente de acuerdo con los principios de protección de datos definidos en la legislación correspondiente. Por lo tanto, la legislación nacional sobre protección de datos seguirá siendo aplicable a las empresas responsables del tratamiento de datos personales[177]. Además, los Estados miembros podrían aplicar reglamentos encarnados en la Directiva sobre telecomunicaciones y que amplíen los requisitos de la Directiva sobre comercio electrónico, es decir, las comunicaciones comerciales podrían quedar sujetas al consentimiento previo del destinatario[178].

IV. Conclusiones

Las normas establecidas en la Directiva general, la Directiva sobre comercio electrónico, la Directiva sobre venta a distancia y la Directiva sobre telecomunicaciones son aplicables al uso de correo electrónico comercial con fines de cibermarketing.

---

[172] Apartado 2 del artículo 12 de la Directiva 97/66/CE.
[173] Apartado 1 del artículo 12 de la Directiva 97/66/CE.
[174] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).
[175] Artículo 7 de la Directiva 2000/31/CE.
[176] Artículo 7 de la Directiva 2000/31/CE.
[177] Artículo 4 de la Directiva 95/46/CE.
[178] Artículo 12 de la Directiva 97/66/CE. Propuesta de Directiva relativa al tratamiento de los datos personales y a la protección de la privacidad en el sector de las telecomunicaciones, artículo 13 relativo a las comunicaciones comerciales no solicitadas.

Sólo la Directiva general se aplica a la elaboración del perfil en línea. Aunque forma parte del comercio electrónico, la elaboración del perfil en línea no se trata en la directiva correspondiente. Además, la Directiva revisada sobre telecomunicaciones tampoco abarca la publicidad en Internet, pues los proveedores que prestan este servicio están excluidos explícitamente de su alcance.
Por lo tanto, se pueden extraer las siguientes conclusiones:

Elaboración del perfil en línea y publicidad[179]

- Los *proveedores de servicios de Internet* deben informar a los usuarios antes de recoger sus datos sobre el tratamiento que se les quiere aplicar[180]. Esto incluye el tipo, el ámbito y la duración del almacenamiento, así como los fines del tratamiento, es decir, su uso para elaboración de perfiles[181]. Si los datos se comunican a terceros, ello se ha de mencionar de forma explícita.
  También se debe informar cuando los datos se recojan utilizando seudónimos o números de identificación no personalizados. En particular, se ha de informar a los usuarios antes de la colocación de una *cookie* para elaborar un perfil personal. Esto debería hacerse mediante un cuadro especial (aviso) que se activase incluso si el navegador no notifica al usuario la colocación de la *cookie*.
- En todo momento, y como mínimo, se ha de dar a los usuarios el derecho a negarse al tratamiento de sus datos[182]. En ese caso, los datos recabados durante el uso de Internet no se deberán usar para ampliar un fichero existente, lo que también es aplicable cuando el tratamiento esté sujeto al consentimiento previo del usuario.
- La personalización de perfiles ha de estar sujeta a la información y al consentimiento previo de los interesados, que deberán tener derecho a retirar su aprobación en cualquier momento y con efecto futuro.
- Los usuarios han de tener en todo momento la oportunidad de acceder a sus perfiles para inspeccionarlos y han de gozar del derecho de corregir y suprimir los datos almacenados[183].

Correo electrónico comercial

- La empresa que recoja una dirección de correo electrónico *directamente a partir del usuario* con vistas a enviar mensajes electrónicos comerciales o a que lo haga un tercero al que comunique la dirección tiene que informar al usuario, utilizando los medios técnicos adecuados, de los objetivos que perseguía cuando recabó la dirección[184].
- Mientras los Estados miembros puedan elegir entre el consentimiento y la oposición a la recepción de mensajes electrónicos comerciales, las empresas que envíen mensajes electrónicos comerciales deberán asegurarse, utilizando los medios técnicos adecuados, de que el usuario pueda identificar como tales dichos mensajes[185].
- Mientras los Estados miembros puedan elegir entre el consentimiento y la oposición a la recepción de mensajes electrónicos comerciales, antes de enviar uno de estos

[179] Estas conclusiones se basan en la decisión alcanzada por la autoridad alemana de protección de datos relativa a un anunciante específico de la red. El Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones adoptó una posición común que también refleja esta decisión. Véase http://www.datenschutz-berlin.de/doc/int/iwgdpt/pr_en.htm.
[180] Artículo 10 de la Directiva 95/46/CE.
[181] Artículo 6 de la Directiva 95/46/CE.
[182] Artículo 14 de la Directiva 95/46/CE.
[183] Artículo 12 de la Directiva 95/46/CE.
[184] Artículo 10 de la Directiva 95/46/CE.
[185] Artículo 7 de la Directiva 2000/31/CE.

mensajes la empresa deberá consultar los registros donde figuren los usuarios que hayan optado por oponerse. Estos registros se han de respetar en todos los casos[186]. La existencia de registros internacionales de los usuarios que no desean recibir este tipo de mensajes sería muy beneficiosa.

- La recogida de direcciones de correo electrónico *en espacios públicos de Internet* y su utilización para enviar mensajes comerciales va en contra de la legislación comunitaria pertinente, es decir, de la Directiva general[187]. En primer lugar, esta práctica constituye un tratamiento ilegal de datos personales[188]; en segundo lugar, va en contra del principio de finalidad[189], pues los usuarios publican su dirección personal con un fin específico, como participar en un foro de debate, muy diferente de la recepción de mensajes electrónicos comerciales; en tercer lugar, no se puede considerar que satisface el criterio del equilibrio de intereses[190], pues el destinatario sale perdiendo en cuestión de tiempo y dinero y sufre molestias irrazonables.
- Cinco Estados miembros (Alemania, Austria, Italia, Finlandia y Dinamarca) han adoptado medidas dirigidas a prohibir las comunicaciones comerciales no solicitadas. En algunos de los Estados miembros restantes existe un sistema de oposición a la recepción de dichos mensajes; en otros, la situación no está muy clara. Las empresas de los países que disponen de tal sistema de oposición pueden enviar mensajes no sólo a direcciones de correo electrónico de su propio país, sino también a consumidores de otros Estados miembros donde exista un sistema de consentimiento. Además, al ser frecuente que las direcciones de correo electrónico no indiquen el país de residencia de los destinatarios, un sistema de regímenes divergentes dentro del mercado interior no proporciona una solución común para proteger la privacidad del consumidor. Por lo tanto, el sistema de consentimiento es una solución bien equilibrada y eficaz para suprimir los obstáculos a la transmisión de comunicaciones comerciales al mismo tiempo que se protege el derecho fundamental de privacidad de los consumidores. Así pues, el Grupo de Trabajo acoge favorablemente y apoya la propuesta de tratar los mensajes electrónicos no comerciales de la misma manera que los aparatos de llamada automática y los facsímiles. En todas estas situaciones, el abonado no cuenta con un interlocutor humano y corre como mínimo con una parte de los costes de la comunicación. El grado de invasión de la privacidad y la carga económica son comparables[191].

[186] Artículo 7 de la Directiva 2000/31/CE.

[187] Véase el Dictamen 1/2000 sobre determinados aspectos de protección de datos del comercio electrónico, presentado por el Grupo operativo sobre Internet (WP 28).

[188] Letra a) del primer apartado del artículo 6 de la Directiva 95/46/CE.

[189] Letra b) del primer apartado del artículo 6 de la Directiva 95/46/CE.

[190] Letra f) del artículo 7 de la Directiva 95/46/CE.

[191] Véase el Dictamen 7/2000 sobre la propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la privacidad en el sector de las comunicaciones electrónicas, de 12 de julio de 2000, COM (2000) 385, adoptado el 2 de noviembre de 2000, WP 36.

CAPÍTULO 9: MEDIDAS EN FAVOR DE LA PRIVACIDAD

I. Introducción

La Directiva comunitaria sobre protección de datos contiene dos principios con consecuencias directas en el diseño y el uso de nuevas tecnologías:
- Su "principio de finalidad" exige que los datos personales se utilicen únicamente cuando sea necesario con un fin específico legítimo; es decir, no se permite el uso de los datos personales sin una razón legítima, y el individuo guarda el anonimato (letra b del primer apartado del artículo 6 y artículo 7).
- Su "principio de seguridad de los datos" exige que los responsables del tratamiento apliquen medidas de seguridad apropiadas a los riesgos que afectan al almacenamiento o la comunicación de los datos personales, con vistas a protegerlos contra la destrucción accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento conlleve la transmisión de datos dentro de una red, y contra otra forma ilícita de tratamiento (artículo 17).

El principio de "finalidad" mencionado es el motivo subyacente del concepto de tecnologías de protección de la privacidad, que se refiere a una serie de tecnologías que salvaguardan la privacidad personal, sobre todo minimizando o eliminando la recogida o el tratamiento de datos identificables[192].
Las tecnologías de protección de la privacidad intentan obstaculizar cualquier forma ilegal de tratamiento, por ejemplo haciendo técnicamente imposible que personas no autorizadas accedan a datos personales, con lo que se evita la destrucción, la alteración y la revelación de tales datos.
La aplicación práctica de este concepto requiere soluciones organizativas y técnicas.

A menudo estas tecnologías se basan en el uso de un protector de la identidad[193], que se puede considerar un elemento del sistema que controla la divulgación de la identidad verdadera de una persona en diversos procesos del sistema de información. Su efecto es el acordonamiento de determinadas áreas del sistema que no requieren acceso a la identidad verdadera. Una de las funciones más importantes del protector de la identidad es la de convertir la identidad real de un usuario en una seudoidentidad, una identidad sustitutiva (digital) que el usuario puede adoptar cuando utiliza el sistema.
Para introducir un protector de la identidad en un sistema de información se pueden utilizar varias técnicas, entre las que encontramos las de *encriptación* con *firmas electrónicas*, firmas ciegas, seudónimos electrónicos y *terceros de confianza*.

II. Tecnologías en favor de la privacidad

Este apartado describe y analiza diversas tecnologías en favor de la privacidad[194].

[192] Véase el informe de HES, R. y BORKING, J. (editores), *Privacy-enhancing technologies: the path to anonymity (revised edition)*, Registratiekamer, en colaboración con el Comisario de información y privacidad de Ontario, Achtergrondstudies en Verkenningen 11, La Haya, noviembre de 1998. Disponible en www.registratiekamer.nl.
[193] Para obtener más detalles, véase el informe de la Registratiekamer sobre las tecnologías de protección de la privacidad *(op cit.)*, y en particular sus páginas 7 y ss.
[194] Véase también la guía EPIC en línea sobre herramientas prácticas de privacidad, disponible en www.epic.org/privacy/tools.html.

Anuladores de *cookies*

A continuación se analizan dos tipos diferentes de respuesta a los problemas de privacidad que suscitan las *cookies*. El primero surgió de la propia industria de Internet y se ha incorporado a los principales navegadores del mercado, mientras que el segundo procede de diversos grupos defensores de la privacidad o empresas de software y consiste en una serie de herramientas que permiten borrar todas las *cookies* o una parte de ellas.

Mecanismos de oposición a las cookies *utilizados por la industria*

El único intento visible de resolver el problema de las *cookies* es el mecanismo de oposición a las *cookies* utilizado a partir de la versión 3 de los navegadores más extendidos. Al configurar el navegador, el usuario precavido puede elegir entre tres opciones:

– Aceptar todas las *cookies.*
– Rechazar todas las *cookies* o las *cookies* que no se vuelven a enviar al servidor de origen (Netscape).
– Ser consultado en cada caso.

No obstante, los mecanismos de oposición a las *cookies* siguen siendo insuficientes por muchos motivos:

1. Normalmente, la configuración por defecto (aceptar todas las *cookies*) es la que más invade la privacidad, y el usuario medio de Internet ignora el amplio uso que las empresas de cibermarketing, por ejemplo, hacen de las *cookies* para rastrear palabras clave en motores de búsqueda a través de medios invisibles de tratamiento.
2. El mecanismo de bloqueo de *cookies* impide la recepción de nuevas *cookies*, pero no el envío sistemático e invisible de las *cookies* que ya se han recibido.
3. Las *cookies* pueden presentar naturalezas muy diferentes: algunas resultan útiles y no son identificativas (por ejemplo, la lengua preferida); otras son identificativas pero pueden respetar las reglas de privacidad. En general, se puede decir que las *cookies* de sesión[195] son mucho menos invasivas de la privacidad que las duraderas. Al usuario de Internet podría no interesarle rechazar todas las *cookies*.
4. Ciertos sitios web deniegan el acceso a los usuarios que no quieren aceptar *cookies*.
5. Ciertos sitios web (sitios web con *hipervínculos* invisibles) envían series de *cookies*. Un enfoque caso por caso obliga al usuario a rechazar cada una de ellas una tras otra, lo que origina una "fatiga del clic" que lleva al usuario a aceptar la *cookie* para que no lo interrumpan más.
6. En algunos casos, el mensaje que transmite la *cookie*[196] parece estar incompleto y puede inducir a error.
7. Al instalar un navegador, el primer sitio que se visite (por defecto, el sitio del fabricante del navegador) puede enviar una *cookie* antes de que el usuario haya tenido la oportunidad de desactivar la aceptación de *cookies*.

En julio de 2000, Microsoft anunció que en la siguiente versión de Internet Explorer iba a introducir la versión beta de un programa complementario de seguridad que permitiría gestionar mejor las *cookies* de la red[197]. Según las primeras descripciones, este programa incluirá diversas características que permitirán a los usuarios controlar mejor las *cookies*.

[195] Las *cookies* sin duración fija no se almacenarán en el disco duro, sino sólo en la memoria RAM.

[196] En MSIE 4.O UK, los avisos de *cookies* están redactados como sigue: *"¿Permite que este sitio web introduzca información en su ordenador para obtener una experiencia navegadora más personal? Si pulsa el "Sí", el sitio web guardará un fichero en su ordenador. Si pulsa el "No", la página web actual puede no mostrarse correctamente"*. El usuario debe entonces pulsar otro botón para conocer el dominio (no el emisor) de la *cookie* y su duración.

[197] EPIC Alert 7.14, 27 de julio de 2000.

El navegador será capaz de diferenciar entre las *cookies* procedentes del interlocutor y las de terceras partes, y la configuración por defecto advertirá al usuario cuando se esté instalando una *cookie* duradera procedente de terceras partes. Además, la nueva funcionalidad permitirá a los usuarios de Internet suprimir todas las *cookies* con un simple clic y dará un acceso más fácil a la información sobre seguridad y privacidad. Sin embargo, este programa complementario de seguridad no aumenta el control del consumidor sobre el uso de *cookies* del interlocutor, frecuentes en los sitios web comerciales.

Programas independientes

"Cookie washer", "Cookie cutter", "Cookie master" y "Cookie cruncher" son algunos de los programas de software gratuito o *software compartido* que todo usuario puede descargar y utilizar en la red[198]. Sobre ellos se pueden formular comentarios similares a los anteriores:

1. El usuario de Internet ha de tratar sus propios ficheros *cookies* a diario y caso por caso debido a las diferentes naturalezas de las *cookies*.
2. En el caso de programas de *software compartido*, en ocasiones el usuario de Internet ha de pagar por protegerse.
3. El mecanismo de manejo de *cookies* no es siempre fácil de utilizar o de comprender para un usuario medio de Internet.

Servidores proxy

El *servidor proxy* es un servidor intermediario entre el usuario de Internet y la Red. Actúa como una *caché web* y mejora de un modo extraordinario el funcionamiento de Internet, por lo que muchas grandes organizaciones o proveedores de acceso a Internet ya han aplicado esta solución. Cada página, imagen o logotipo descargado desde el exterior por un miembro de una organización se almacena en una caché en el *servidor proxy* y queda automáticamente disponible para los otros miembros de la misma organización.

En este caso no es necesario que cada miembro de la organización situado ante el *servidor proxy* tenga su propia dirección IP, pues no accede directamente a Internet. Además, normalmente el *servidor proxy* no transmitirá[199] la dirección IP del usuario de Internet al sitio web y puede filtrar el charloteo del navegador. Dado que el *servidor proxy* maneja el *protocolo* HTTP, puede suprimir, cambiar o almacenar fácilmente las *cookies* almacenadas en la cabecera HTTP.

Software que garantiza el anonimato

Estos programas permiten a los usuarios interactuar de forma anónima cuando visitan sitios web, pues primero pasan por un sitio que garantiza su anonimato disfrazando su identidad[200].

Deteniéndose en un sitio web que garantiza el anonimato antes de ir a ningún otro, el usuario puede permitir que se oculten datos personales, como su dirección IP, al sitio web que visite. Los sitios de anonimato bloquean también el envío de datos del sistema (como el sistema operativo y el navegador que se están utilizando) a los sitios web, impiden se instalen *cookies* en los navegadores y bloquean los módulos *Java* y *JavaScript*, que en otro caso pueden acceder a datos personales de los navegadores.

---

[198] Algunos de estos programas pueden encontrarse en http://tucows.belgium.eu.net/cookie95.html.

[199] Lamentablemente, algunos *proxies* añaden a la cabecera HTTP la dirección TCP-IP del PC para el que están trabajando.

[200] Véase el libro "Net Worth" *(op. cit.)*, páginas 273 y ss.

Anonymizer [201] y Zero Knowledge System [202] son dos buenos ejemplos de ello.

Anonymizer pretende:

- actuar como un intermediario entre el usuario y los sitios que visita, ocultando su identidad ante medidas invasivas de rastreo;
- bloquear los programas incluidos en la página web (*Java* y *JavaScript*) que pueden dañar el ordenador del usuario o reunir datos personales confidenciales.

Anonymizer ofrece dos servicios (la navegación anónima y el correo electrónico anónimo) y un producto (el servidor que garantiza el anonimato), que permite a cualquier usuario crear un sitio propio que garantice el anonimato.

En ocasiones, el usuario de Internet ha de pagar para poder aprovechar plenamente las ventajas de los servicios que garantizan el anonimato. Para poder utilizar los servicios del sitio web de Anonymizer ha de estar continuamente conectado a él, lo que significa que este servicio es muy vulnerable a la vigilancia de terceras partes. Anonymizer puede prestar servicios anónimos como la navegación, el correo o la transferencia de ficheros.

Técnicamente hablando, Anonymizer actúa como un *servidor proxy* y ocultará el charloteo del navegador HTTP y la dirección IP del usuario.

El principal problema que presenta el uso de este servicio es que el usuario de Internet tiene que depositar su confianza en una empresa específica que estará al corriente de cada paso que el usuario dé en la red.

Zero Knowledge System propone un programa denominado "Freedom" que se basa al menos en tres retransmisores TCP/IP combinados con una *encriptación* muy fuerte (de 128 bits como mínimo). Dado que todos los servicios de la red utilizan el *protocolo* TCP/IP, con este sistema todos quedan encriptados y en el anonimato. Cada una de las tres estaciones retransmisoras TCP/IP conoce únicamente la dirección TCP de su predecesora. No llevan ningún fichero registro, por lo que incluso dos retransmisores unidos serían incapaces de rastrear la información solicitada o recuperada. La ruta de la información es, por supuesto, dinámica, y es probable que cambie incluso durante una comunicación muy corta. Parece ser que en Freedom se ha integrado un sistema de gestión de *cookies*.

Otro ejemplo de este tipo de servicios es el que ofrece **privada.com**, empresa que presta servicios de apoyo a todos los tipos de transacciones de la red, incluidos la navegación, el correo electrónico, la mensajería y, pronto, el comercio. La infraestructura de Privada se basa en un sistema de compartimentación y *encriptación*.
El usuario recibe un CD-ROM o descarga una aplicación cliente, PrivadaControl, desde su *proveedor de servicios de Internet*. PrivadaControl se comunica con los servidores de la red de Privada situados en las instalaciones del *proveedor de servicios de Internet* y funciona como un *cortafuegos* para la privacidad personal del usuario. PrivadaControl está orientado a proteger toda la información y los datos de los usuarios desde el punto de la transacción y a través de su camino por la red, garantizando la privacidad del usuario desde todos los puntos de vista, incluido el de Privada y el del *proveedor de servicios de Internet*.
Al usar PrivadaControl, el usuario crea una cuenta electrónica privada que representa sus actividades en línea al tiempo de disocia completamente toda la información personal del usuario de la actividad en línea. PrivadaControl parece permitir que el usuario cree o

[201] http://www.anonymizer.com/3.0/index.shtml.
[202] http://www.zeroknowledge.com.

suprima identidades electrónicas, elija entre ellas mientras interactúa en línea y configure sus propios atributos y características.
Este sistema no bloquea todas las aplicacioncitas en *Java*, *cookies*, o controles ActiveX, pero permite al usuario decidir a qué nivel pueden funcionar la personalización y los servicios de la red. Las *cookies* no se colocan en el ordenador personal del usuario, sino en servidores centralizados de la red Privada. Todos los ficheros históricos o intentos de *minería de datos* por parte de un sitio web están asociados con la identidad del usuario en línea, y no con su identidad real. Privada afirma que los usuarios pueden suprimir fácilmente una o todas las *cookies* que se hayan instalado.

El sistema propuesto por **iPrivacy** está diseñado para permitir el comercio electrónico anónimo, desde navegar, hasta comprar y enviar. Permite a los consumidores navegar, buscar y comprar en la Red de forma privada y recibir lo que hayan comprado sin que se revele la identidad del destinatario. De acuerdo con la empresa, ni siquiera ellos mismos podrían conocer la verdadera identidad de los clientes que hacen uso de sus servicios. En cuanto a la transacción, sólo el cliente y el usuario de la tarjeta de crédito conocerían información personal sobre la compra realizada en línea[203].

Filtros de correo electrónico y correo electrónico anónimo[204]

Estos sistemas ya se han descrito en el capítulo sobre el correo electrónico. Lo que sigue es un resumen de sus rasgos principales:

- Los filtros de correo electrónico examinan los mensajes electrónicos que llegan a un usuario y sólo dejan pasar los que dicho usuario ha indicado que quiere recibir. Se suelen utilizar para descartar la propaganda por correo.

- El correo electrónico anónimo permite a los usuarios ofrecer su dirección de correo electrónico en línea sin tener que revelar su identidad[205]. Actualmente se puede acceder de forma gratuita a este servicio en Internet a través de una serie de empresas que prestan servicios "de reenvío" eliminando la identidad del usuario antes de volver a enviar el mensaje electrónico.

Informediarios

Un usuario puede también decidir utilizar lo que se denomina un informediario[206], que se ha descrito como "una persona de confianza o una organización con acceso a la red especializada en servicios de información y conocimientos destinados a la comunidad virtual, sobre ella y en su nombre. El informediario facilita y estimula la comunicación inteligente y la interacción entre los miembros de dicha comunidad. También administra y cultiva un activo de conocimiento privado con contenido e *hipervínculos* de interés específico para la comunidad. De acuerdo con los condicionantes de la privacidad que exige la comunidad virtual, el informediario reúne, organiza y libera de forma selectiva información acerca de la comunidad y de sus miembros para cubrir las necesidades de la comunidad virtual…".

[203] http://www.iprivacy.com.
[204] Véase el libro "Net Worth" *(op. cit.)*, páginas 275 y ss.
[205] Este tipo de servicios se comentan también en el apartado sobre medidas en favor de la privacidad del capítulo 6, "Publicaciones y foros".
[206] http://www.fourthwavegroup.com/Publicx/1635w.htm.

El informediario es un nuevo tipo de intermediario empresarial que ayuda a los clientes a captar, gestionar y maximizar el valor de sus datos personales[207]. Los consumidores han demostrado que están dispuestos a dar información personal siempre y cuando puedan sacar algún provecho de ello, aunque cada vez se dan más cuenta de que están vendiendo su privacidad a un precio muy bajo a empresas que la utilizan en beneficio propio. Lo que consiguen gracias a la información que divulgan es, en una palabra, insatisfactorio[208].

Los informediarios podrían ayudar a los consumidores a cerrar mejores tratos con los vendedores, agregando sus datos a los de los consumidores y usando su poder de mercado conjunto para negociar por su cuenta con los vendedores. Actúan como guardianes, agentes y corredores de información de los consumidores, vendiéndola a empresas (y ofreciéndoles acceso a ella) en nombre del consumidor, al mismo tiempo que protegen sus datos personales del abuso.

El aspecto positivo de los informediarios es que, en muchos casos, pueden comprar los bienes o servicios que desean y hacerlos llegar al consumidor final sin que éste salga del anonimato. También pueden proporcionar agentes inteligentes que ayuden a los abonados a cumplir su tarea.

En teoría, los clientes de los informediarios tendrán la opción de seguir en el anonimato mientras navegan por la Web y realizan compras en línea. Sin embargo, se les instará a que no lo hagan, pues cada vez que accedan a divulgar su identidad o su dirección de correo de electrónico, los vendedores les pagarán una pequeña cuota o les aplicarán un descuento en el precio del producto vendido.

Los clientes también recibirán pagos en metálico si dan a determinadas empresas acceso a su perfil personal. El importe del pago dependerá de las preferencias de privacidad de cada cliente. Quienes elijan seguir en el anonimato total renunciarán a los pagos en metálico, a cambio de la garantía de su privacidad, mientras que quienes acepten los controles impuestos por el intermediario sobre el acceso a su información y entiendan el interés de una revelación selectiva pueden ganar dinero.

En conclusión, se puede afirmar que si un informediario puede desempeñar una papel positivo a la hora de proteger los datos de los usuarios con los que mantiene una relación de confianza, la base de este acuerdo es la posibilidad de generar beneficios divulgando los datos personales de los clientes y dando acceso a ellos.

Según las circunstancias y la naturaleza del informediario, éste puede ser tanto un protector de la privacidad como un invasor de la misma.

III. Otras medidas en favor de la privacidad

También se pueden utilizar otras técnicas para mejorar la transparencia del tratamiento o facilitar el ejercicio de los derechos del interesado. A continuación se dan algunos ejemplos:

[207] Uno de los estudios más completos sobre este nuevo órgano es el libro *"Net Worth: the emerging role of the infomediary in the race for customer information"*; HAGEL III, J. y SINGER, M., Harvard Business School Press.
[208] HAGEL III, J. y SINGER, M. *(op. cit)*.

P3P

P3P significa Plataforma de Preferencias de Privacidad[209]. Su objetivo es permitir que los sitios web expresen sus preferencias de privacidad y los usuarios ejerzan sus preferencias sobre estas prácticas, de forma que puedan tomar decisiones con conocimiento de causa sobre sus experiencias en la Web y controlar el uso de su información. Toda la comunidad de protección de datos ha seguido el desarrollo de la P3P con gran interés.

En abril de 1998, el Grupo Internacional de Trabajo sobre protección de datos en el ámbito de las telecomunicaciones emitió una posición común sobre los puntos esenciales de las tecnologías en favor de la privacidad (por ejemplo, P3P) en la World Wide Web[210]. Este documento establece las condiciones esenciales que ha de satisfacer cualquier plataforma técnica para la protección de la privacidad en la World Wide Web, con el objetivo de evitar la recogida sistemática de datos personales:

1. La tecnología en sí misma no puede garantizar la privacidad en la Web y se ha de aplicar siguiendo un marco normativo.
2. Cualquier usuario debería tener la posibilidad de navegar de forma anónima, lo que también es aplicable a la descarga de información del dominio público.
3. Antes de que un proveedor de sitios web trate datos personales, y sobre todo los revelados por el usuario, se ha de obtener el consentimiento fundamentado de éste. Además, en la configuración por defecto de la plataforma técnica se deberían introducir ciertas reglas de base ineludibles.

Dos meses más tarde, en junio de 1998, el Grupo de Trabajo emitió también un dictamen[211] que hacía hincapié en que una plataforma técnica de protección de la privacidad no sería suficiente, por sí sola, para proteger la privacidad en la Web. La plataforma se ha de aplicar en el contexto de un marco de normativas aplicables sobre protección de datos que proporcionen un nivel mínimo, no negociable, de protección de la privacidad para todas las personas. El dictamen mencionaba asimismo una serie de cuestiones específicas que surgirían con la aplicación de tal sistema en la Unión Europea.

En septiembre de 1999 se organizó un seminario conjunto para investigar la aplicación de la P3P en el contexto de la Directiva europea sobre protección de datos y fomentar la comunicación entre la comunidad de protección de datos de la UE y los desarrolladores de software. En el seminario participaron una delegación de alto nivel del W3C y miembros del Grupo operativo sobre Internet. En él se demostró que todavía se ha de tratar un buen número de cuestiones.

Una vez que se solucionen, la P3P podría desempeñar un papel positivo si se aplica en el marco adecuado. Los principales aspectos positivos de la P3P son los siguientes[212]:

- La P3P puede ayudar a normalizar los avisos relacionados con la privacidad. Aunque en sí mismo esto no puede proteger la privacidad, si se ejecuta podría proporcionar mucha más transparencia y utilizarse para apoyar los esfuerzos por mejorar la protección de la privacidad.

---

[209] El último borrador de trabajo del *protocolo* P3P se puede consultar en el sitio web del W3C, en http://www.w3.org/TR/1999/WD-P3P.

[210] Este texto está disponible en: http://www.datenschutz-berlin.de/doc/int/iwgdpt/priv_en.htm.

[211] Dictamen 1/98: Plataforma de Preferencias de Privacidad (P3P) y Norma de Perfiles Abierta (OPS), adoptado el 16 de junio de 1998, WP 11, XV D/5032/98.

[212] Véase el artículo de CAVOUKIAN, A. y GURSKI, M. (Comisario de información y privacidad de Ontario) y MULLIGAN, D. y SCHWARTZ, A. ("Center for Democracy and Technology"), *P3P and privacy: an update for the Privacy Community*, disponible en: wysiwyg://16/http://www.cdt.org/privacy/pet/p3pprivacy.

- La P3P puede apoyar el aumento de las posibilidades de privacidad, incluidos el anonimato y el uso de seudónimos.

Sin embargo, conviene ser consciente de las limitaciones[213] de la P3P:

- La P3P no puede proteger a los usuarios en países cuya legislación sobre la privacidad es insuficiente, pues no puede crear medidas públicas ni exigir que sus especificaciones se sigan en el mercado.
- La P3P no puede garantizar que las empresas sigan las políticas de privacidad. De hecho, no puede garantizar que el sitio esté haciendo lo que afirma hacer. Las sanciones por incumplir una declaración de intenciones sólo pueden establecerse por ley o mediante la adhesión a un organismo autorregulador.

La etiqueta de privacidad

Se trata de un sello de calidad que se impone a un sitio web. A lo largo de los años han aparecido diversas etiquetas de privacidad, entre las que destacan las de TRUSTe[214], Privaseek[215], Better Business Bureau[216] y WebTrust[217]. Algunas de estas organizaciones estadounidenses opera en el ámbito internacional, incluida Europa; otras aspiran a hacerlo. Al mismo tiempo, en Europa están surgiendo iniciativas similares con fines internacionales, por ejemplo L@belsite en Francia.

Las etiquetas de privacidad se otorgan a las empresas que cumplen una serie de requisitos especificados por el organismo que las concede, que puede ejercer algún tipo de control sobre el cumplimiento de las políticas de privacidad de las empresas que las poseen mediante revisiones periódicas de sus actividades. En algunos casos, el organismo que concede la etiqueta se encarga también de las quejas presentadas contra empresas que tienen la etiqueta en sus sitios web.

La etiqueta de privacidad plantea una serie de cuestiones:

1. La primera se refiere al contenido de la etiqueta. El derecho a la información y al acceso, el principio de minimización de datos, el derecho a oponerse, el principio de legitimidad y proporcionalidad y la obligación de notificar a la autoridad nacional de protección de datos son algunas de las piedras angulares de los principios europeos de protección de datos. El principal riesgo social sería la difusión de etiquetas de privacidad en toda Europa, lo que confundiría a los usuarios y a los responsables del tratamiento. Aunque pueden dar esta impresión, no todas las etiquetas garantizan seriamente todos los principios de protección de datos mencionados.

2. El segundo problema radica en el control de las prácticas de privacidad de los sitios web. Se pueden practicar numerosos tipos de control. Algunas de las principales preocupaciones al respecto son:

- ¿Quién tiene el control? ¿Cómo lo ejerce? ¿Con qué clase de mandato otorgado por la empresa controlada? En el peor de los casos, parece que el responsable del tratamiento será, principalmente, el propio interesado, con todos los problemas que esto conlleva a la hora de identificar los fallos en la observación de las prácticas de privacidad declaradas, demostrarlos y notificarlos a la empresa que asigna las etiquetas. Además, no todos los organismos que conceden etiquetas pueden garantizar que las empresas actúen según pretenden sus políticas.

[213] Véase la nota al pie anterior.
[214] http://www.truste.org.
[215] http://www.privaseek.com
[216] http://www.bbbonline.org/businesses/privacy/index.html.
[217] http://www.cpawebtrust.org/consumer/index.html.

- ¿Quién pagará? Dado que la asignación de etiquetas es una iniciativa privada que a menudo no cuenta con apoyo económico gubernamental, algunos organismos que conceden etiquetas sufrirán la presión de las empresas que supuestamente controlan.
- ¿Qué sanciones se impondrán, si se impone alguna?

Sin embargo, no se deben subestimar los posibles efectos de las etiquetas de privacidad en la protección de ésta, pues pueden ayudar a concienciar a los usuarios de Internet sobre la privacidad. Se pueden formular algunas propuestas para abordar los problemas mencionados:

1. El contenido de la etiqueta: Con el fin de garantizar que las etiquetas de privacidad cumplen las normas de la legislación europea sobre protección de datos, el Grupo de Trabajo podría acordar una norma europea de etiquetas de privacidad con los requisitos que debe cumplir una etiqueta[218].

Mientras los usuarios de Internet tengan claro qué etiquetas son las que cumplen las normas europeas, pueden coexistir varias.

2. El control de las prácticas de privacidad del sitio web: La fiabilidad de las prácticas de privacidad del sitio web podría mejorar considerablemente si se obligase a los sitios dotados de una etiqueta a someterse a auditorías periódicas. La norma europea de etiquetas de privacidad podría incluir este requisito y determinar posibles formas de llevar a cabo estos controles obligatorios: auditoría realizada por el propio sitio con la ayuda de una lista de control, auditoría realizada por terceros, etc.

IV. Conclusiones

- Se deberían emitir recomendaciones sobre el diseño de navegadores conformes a la protección de la privacidad y cuya configuración por defecto respete la privacidad al máximo.
- Los *servidores proxy* anónimos pueden ocultar la dirección IP. Todos los *proveedores de servicios de Internet* los podrían ofrecer como un elemento gratuito estándar con cada suscripción a Internet.
- Los sitios web no deberían denegar el acceso a los usuarios que no quieran aceptar *cookies*, a menos que sean indispensables *cookies* de sesión para establecer un vínculo entre el usuario y sus diversas compras en la red y hacer así posible que la facturación se realice de forma adecuada.
- Se debería fomentar el uso de tecnologías a favor de la privacidad, especialmente si quienes las instalan son los *proveedores de servicios de Internet* u otros agentes.
- Parece ser que los usuarios necesitan más información sobre la existencia de tecnologías en favor de la privacidad. El sector público debería dar los pasos necesarios para concienciar más sobre este tema y apoyar el desarrollo de este tipo de soluciones, además de utilizarlas y fomentarlas[219].

[218] La autoridad francesa para la protección de datos (CNIL) ha realizado un trabajo muy interesante en este ámbito que podría servir para inspirar la norma europea. Véase www.cnil.fr.

[219] En los Países Bajos se aprobó una moción durante el debate parlamentario sobre la nueva legislación de protección de datos en la Segunda Cámara, por la que se pidió al Gobierno que fomentase el desarrollo y el uso de las tecnologías de protección de la privacidad y que instase al sector público a tomar la iniciativa como promotor de este tipo de tecnologías en su propio tratamiento de datos personales. Moción número 31 de NICOLAÏ C.S., presentada el 18 de noviembre de 1999 con relación al proyecto de ley 25 892 (*Regels inzake de bescherming van persoonsgegevens, Wet bescherming persoonsgegevens*), La Haya, Tweede Kamer, vergaderjaar 1999–2000, 25 892, nº 31.

- El Grupo de Trabajo podría acordar una norma europea sobre etiquetas de privacidad que debería incluir la obligación de que los sitios web se sometan a auditorías periódicas.

CAPÍTULO 10: CONCLUSIONES

En este documento se ha abordado una serie de temas presentados en capítulos separados. Cada uno de ellos incluye comentarios exclusivos sobre cuestiones concretas. Sin embargo, ciertas cuestiones comunes que guardan relación con todos los servicios de Internet descritos en el documento merecen tratarse en términos más generales.
Tras resumir las tendencias y de los riesgos de la privacidad que se han observado en los diversos aspectos del uso de Internet, se ha intentado ofrecer algunas directrices y recomendaciones, teniendo en cuenta acciones que podrían desarrollarse a varios niveles.

1. Tendencias y riesgos

El desarrollo de Internet es exponencial. El usuario de Internet dispone de un número cada vez mayor de servicios, desde realizar compras en línea hasta participar en foros con gente de todo el mundo. Debido a la complejidad de la Red, cada ver resulta más difícil formarse una visión general de todas las posibilidades que se ofrecen al usuario. Las empresas buscan una forma de atraerlo y destacarse de otras ofreciendo servicios personalizados y/o gratuitos.
La personalización de los servicios depende de la utilización de datos personales de los usuarios, que las empresas tratan de conseguir de diversas formas, como animar a los propios usuarios a que los proporcionen en el marco de programas de fidelidad, hacerles regalos o prestarles servicios gratuitos, recogerlos de fuentes públicas, etc.
Los perfiles que se elaboran no sólo son valiosos para las empresas que quieren dirigirse al consumidor, sino que además tienen un valor económico en sí mismos, pues a menudo se venden y alquilan a otras empresas.

El desarrollo de nuevas tecnologías facilita el seguimiento de los usuarios de Internet. Por ejemplo, cuando un consumidor utiliza un teléfono móvil para conectarse a Internet se pueden generar datos que indiquen su situación.
Cuando el usuario se conecta a Internet a través de nuevos medios como las líneas *ADSL* o el cable, se le asigna una dirección IP estática que facilita su rastreo de una sesión a otra. Las nuevas generaciones de software y hardware ofrecen características que aumentan la capacidad de controlar las actividades del usuario en tiempo real, a menudo sin que ellos mismos lo sepan. En todo este documento se dan numerosos ejemplos de tratamiento invisible y programas E.T.
En este contexto, el usuario medio cada vez tiene más difícil mantenerse en el anonimato mientras navega por la red.

La combinación de estas capacidades en desarrollo conlleva nuevos riesgos para la privacidad del usuario de Internet, sobre todo cuando los datos están concentrados en las manos de uno o de pocos responsables del tratamiento.
Cuando los responsables del tratamiento utilizan las tecnologías de *minería de datos*, por ejemplo, técnicamente no sólo tienen la posibilidad de tratar y reorganizar los datos, sino también de descubrir nuevos vínculos y características relacionadas con su titular, que normalmente no es consciente de esta posibilidad y no espera que se trate esa información.
Estos riesgos se deben también a que algunos datos se conservan en línea durante un período muy largo de tiempo; por ejemplo, son muchos los mensajes enviados a los foros de debate y las listas de correo que se conservan durante varios años y se pueden consultar mediante herramientas de búsqueda inversa.

Esta disponibilidad de datos personales permite usos secundarios inesperados que suelen ser incompatibles con el fin para el que se recabaron en principio.

2. Directrices y recomendaciones

2.1. Concienciación del usuario de Internet

Dado que, como ya se ha mencionado, los riesgos para la privacidad del usuario son cada vez mayores, resulta especialmente importante garantizar que se utilizan medios adecuados a la hora de garantizar que éste recibe toda la información que precisa para

tomar una decisión con conocimiento de causa. En este proceso de informar al usuario participan varios agentes.

En primer lugar, cualquier responsable del tratamiento que recabe datos personales debe proporcionar al interesado toda la información necesaria. Dicha información, mencionada en el artículo 10 de la Directiva 95/46/CE, ha de proporcionarse en todos los casos en el momento en que se produzca la recogida de datos. Aunque un sitio web haga pública su política de privacidad, lo que resulta útil para que el público esté informado, cada vez que se recojan datos se ha de informar a su titular de una forma simple y accesible; por ejemplo, en la misma pantalla en la que se han de introducir los datos o mediante un cuadro de diálogo.

Cuando el responsable del tratamiento es una empresa privada, el cumplimiento de estas normas no es sólo importante en términos legales, sino también para sus propios intereses, pues propiciará una mayor confianza de los usuarios, lo que podría repercutir en la implicación de éstos en la empresa. En cuanto al desarrollo del comercio electrónico, por ejemplo, se observa que cuando los usuarios temen que sus datos personales no van a contar con una protección y una seguridad correctas se muestran reacios a emprender transacciones electrónicas.

Si el responsable del tratamiento es una autoridad pública, el cumplimiento de las normas de protección de datos es un elemento clave, pues su comportamiento dará ejemplo al público en general. Por ejemplo, las autoridades públicas que realizan actividades electrónicas gubernamentales deberían basarse en la privacidad como una de las piedras angulares del sistema de intercambio de datos. Además, incluso cuando no desempeñan el papel de responsable del tratamiento, la responsabilidad de estas autoridades reside en la educación general y la información del público.
En particular, a las autoridades de protección de datos se les ha confiado la tarea de concienciar a la población sobre los riesgos relacionados con el uso de Internet, pero también sobre los derechos y las obligaciones que prevé la legislación. Esto se puede conseguir de diferentes formas, como la publicación de folletos, informes, comunicados de prensa y recomendaciones prácticas incluidas en las solicitudes de notificación, así como mediante la organización de conferencias o seminarios sobre estos asuntos, dirigidos a los diferentes agentes y sectores de la sociedad, o la participación en ellos.

Tradicionalmente, los defensores de la privacidad han asumido la función de la concienciación pública y en ocasiones sus esfuerzos han conducido a mejoras significativas del respeto de la privacidad de los productos de Internet.
En varios países de la Unión Europea se ha observado que las asociaciones de consumidores tienen una participación y un interés crecientes en las cuestiones relacionadas con la privacidad de las actividades de los consumidores. Este papel puede ser especialmente positivo, ya que no se limita a proporcionar información, sino que además incluye la representación de los consumidores en su relación con las empresas o las autoridades públicas. Estas asociaciones, por ejemplo, pueden controlar que los *proveedores de servicios de Internet* cumplan la ley, o informar a las autoridades públicas de las quejas que reciben sobre un sitio web concreto o sobre una empresa de Internet.
Las asociaciones profesionales también pueden influir positivamente informando a los nuevos agentes sobre sus obligaciones legales.

Todas las partes aquí mencionadas desempeñan un papel significativo a la hora de facilitar al consumidor la información que necesita para poder tomar decisiones

responsables. Por lo tanto, corresponde al usuario utilizar los medios de que dispone para garantizar el respeto de sus derechos y, posiblemente, dejar claro que no aceptará servicios o productos que no respeten el marco legal existente.

2.2. Aplicación de la legislación existente de una forma coherente y coordinada

La protección de datos en línea sólo puede tener las garantías suficientes si se respeta el marco legal vigente. Teniendo en cuenta el carácter internacional de la red, es esencial que los responsables del tratamiento puedan confiar en que se realice una interpretación y una aplicación coherentes y coordinadas de las normas de protección europeas, lo que no sólo es importante de cara a los titulares y a los responsables del tratamiento de datos de la UE, sino también para todos los que residen fuera de la UE y han de tener en cuenta este marco legal, sobre todo a la hora de recabar datos personales utilizando medios situados dentro de la Unión. En este contexto, el Grupo de Trabajo desempeña un importante papel.

El Grupo de Trabajo ha identificado en diversas ocasiones lagunas o cuestiones polémicas en la legislación existente y ha publicado documentos que proporcionan una interpretación común y posibles soluciones. Se ha prestado una especial atención a la revisión de la Directiva 97/66/CE, que ha conllevado mejoras significativas en el ámbito terminológico. Aunque el Grupo de Trabajo considera positivo que en el proyecto de Directiva se hayan tenido en cuenta nuevas cuestiones, se han presentado otras propuestas que también convendría estudiar.

El Grupo de Trabajo está preocupado por el hecho de que las enmiendas a la legislación vigente tiendan en ocasiones hacia la introducción de requisitos legales más estrictos, en particular respecto a las posibilidades de control en la Web y a la generalización de los requisitos de identificación de los usuarios, y ha recordado que, aunque haya otros intereses legítimos en juego, siempre se ha de alcanzar un equilibrio entre éstos y la protección de los datos personales del usuario.

Conviene destacar que la interpretación y la aplicación de la ley no es únicamente tarea de las autoridades públicas, sino que el sector privado puede contribuir de forma muy fructífera invirtiendo en el desarrollo de reglamentos internos o códigos de conducta que aborden cuestiones más concretas surgidas en sectores precisos.

2.3. Desarrollo y utilización de tecnologías en favor de la privacidad, que la respeten y la fomenten

Como ya se ha dicho, el tratamiento de datos personales en Internet depende en gran medida de la configuración técnica del hardware y el software, así como de los *protocolos* y las normas técnicas que se utilicen para la transmisión de la información.
Por lo tanto, resulta especialmente importante tener en cuenta los requisitos de privacidad desde la primera fase del desarrollo de estas herramientas. Por ejemplo, cuando un navegador establece una conexión con un sitio web, no debería transmitir más información que la necesaria. Se insta a quienes participan en el diseño y en el desarrollo de estas herramientas técnicas a que consulten a las autoridades nacionales de protección de datos sobre los requisitos legales existentes en esta cuestión.
Además, para que el público en general tenga claro qué productos respetan la privacidad, sería útil implantar un sistema de marcas de certificación que permitiera un

reconocimiento sencillo de los productos que cumplen los requisitos de protección de datos.

Por otra parte, aunque es frecuente que las nuevas tecnologías se consideren una amenaza para la privacidad, convendría destacar que también representan una herramienta útil de salvaguardia de la misma.

En primer lugar, algunas de las tecnologías existentes pueden utilizarse para mejorar la transparencia y la facilidad de manejo de la información que se proporciona al interesado, por ejemplo dando a los usuarios información simple y accesible en el momento de recabar sus datos personales.
En segundo lugar, pueden constituir una herramienta útil para simplificar el ejercicio de los derechos de los titulares de los datos, por ejemplo permitiendo un acceso directo en línea a los datos personales del usuario o dando la posibilidad de oponerse al proceso.

Si se tiene en cuenta que el usuario medio no está necesariamente familiarizado con los aspectos técnicos del uso de Internet y que no siempre está en situación de decidir sobre la configuración del hardware y el software, ni de cambiarla, es de vital importancia que las configuraciones por defecto de los productos ofrezcan el máximo nivel de protección de la privacidad.

Se ha desarrollado una serie de herramientas adicionales, más conocidas como "tecnologías a favor de la privacidad", para ayudar a los usuarios a salvaguardar su privacidad, sobre todo minimizando o eliminando la recogida o el posterior tratamiento de datos identificables y dificultando técnicamente cualquier forma ilegal de tratamiento. Algunos ejemplos de estas herramientas son los *servidores proxy*, los anuladores de *cookies*, el software que garantiza el anonimato, las herramientas de elaboración de seudónimos (especialmente valiosas en la elaboración de perfiles), los filtros de correo electrónico, etc. Entre los posibles nuevos productos podrían estar las tarjetas inteligentes con un protector portátil de la identidad que el usuario podría introducir en cualquier máquina con la que se conectase en línea.

De todos los agentes mencionados en el apartado 2.1., la industria y el sector público son los primeros que deberían invertir en el desarrollo y la ejecución de tecnologías a favor de la privacidad y fomentarlas. Se debería concienciar al usuario de la existencia de estos medios, que, por otra parte, deberían estar disponibles a precios razonables.

2.4. Establecimiento de mecanismos fiables de control y retroalimentación

Los datos en línea sólo se pueden proteger de forma eficaz si se dispone de los medios adecuados para controlar y evaluar el respeto del marco legal y de los requisitos técnicos explicados anteriormente.
Para lograrlo, aunque las principales encargadas de ese control son las autoridades de protección de datos, otros agentes están tomando medidas dirigidas a la autoevaluación, pues han comprendido el impacto de su política de privacidad en el comportamiento de sus consumidores hacia ellos.
Las autoridades de protección de datos pueden contribuir al desarrollo y al buen funcionamiento de estos sistemas de autoevaluación proporcionando orientación, por ejemplo, en forma de listas de control de autoevaluación normalizadas a escala europea.

Además, se podrían conceder etiquetas para ayudar a los consumidores a conseguir una indicación fiable acerca del respeto de la legislación comunitaria sobre protección de datos en el tratamiento de éstos. El Grupo de Trabajo pretende actuar en este ámbito principalmente para garantizar que las etiquetas de privacidad se asignan a sitios web que respetan esta legislación.

El Grupo de Trabajo invita a todos los agentes que participan en actividades de Internet a que tengan en cuenta este documento de trabajo y den los pasos necesarios para llevar a la práctica sus recomendaciones.

El Grupo de Trabajo espera que este documento de trabajo contribuya a concienciar a los usuarios y que fomente un debate público sobre el tema que, sin duda, requerirá un análisis más profundo y un futuro seguimiento.

GLOSARIO DE TÉRMINOS TÉCNICOS[220]

ADSL

La línea de suscripción asimétrica digital o *ADSL* es un *protocolo* de telecomunicaciones que se puede utilizar con los pares trenzados de cobre clásicos. Permite alcanzar una velocidad de hasta 1 Mbps, mientras que, simultáneamente, la línea permanece libre para una conversación telefónica normal. Las líneas *ADSL* requieren *módems ADSL* dedicados en ambos extremos de la línea local.

Almacén de información

Base de datos diseñada para prestar asistencia a la toma de decisiones en una organización y que puede contener enormes cantidades de datos. Por ejemplo, las grandes organizaciones minoristas pueden tener 100 GB o más de historial de transacciones. Cuando la base de datos está organizada para un departamento o una función, se puede llamar "mercado de datos" ("data mart") en lugar de "*almacén de información*".

Autentificación

Verificación de la identidad de un usuario que se conecta a un sistema informático o verificación de la *integridad* de un mensaje transmitido.

Buzonfia ("spam")

Envío de grandes cantidades de publicidad no solicitada a través del correo electrónico.

Caché web

Sistema informático de una red que guarda, en su memoria o en disco, copias de las páginas web que se han solicitado más recientemente, para agilizar su recuperación. Si la siguiente página que se solicita ya se ha almacenado en la caché, se recupera localmente y no desde Internet. Los servidores de *caché web* están situados en el lado interior del *cortafuegos* de la empresa y permiten que las páginas más solicitadas estén disponibles instantáneamente. Dado que el contenido de las páginas web puede variar, los programas que gestionan la memoria de almacenamiento temporal revisan sin cesar si hay nuevas versiones de la página y las descargan. Tras un período determinado de inactividad, las páginas se borran de la caché.

Certificado electrónico

[220] Algunas de estas definiciones se han extraído de las siguientes fuentes:
- http://www.techweb.com/encyclopedia
- http://webopedia.Internet.com
- *Personal Data Privacy and the Internet: a guide for data users*, Office of the Privacy Commissioner for Personal Data, Hong Kong, 1998.

Un *certificado electrónico* es un documento electrónico que contiene dos grupos de información y que se considera una prueba de identidad en el mundo electrónico. El primer grupo de información es el propio certificado de información, que incluye el nombre o el seudónimo de la persona física o jurídica que solicita el certificado, su clave pública, las fechas de validez del certificado y el nombre la autoridad certificadora. El segundo grupo es la *firma digital* de la autoridad certificadora. Todo el mensaje tiene la *firma digital* de una autoridad certificadora, que goza de la confianza de numerosos servidores (las autoridades certificadoras son un tipo especial de *terceros de confianza)* y puede verificar la relación entre la persona física o jurídica y su clave pública.

Cookies

Las *cookies* son datos que crea un servidor web y pueden almacenarse en ficheros de texto en el disco duro del usuario de Internet, y de los que el sitio web puede conservar una copia. Forman parte del tráfico HTTP, por lo que se pueden transportar sin problemas con el tráfico IP. Una *cookie* puede contener un número único (identificador global único - GUID, "Global Unique Identifier") que permite realizar una mejor identificación que las direcciones IP dinámicas y proporciona al sitio web una forma de rastrear las pautas de comportamiento y las preferencias del usuario.
Las *cookies* contienen una gama de URL (direcciones) para los que son válidas. Cuando el navegador vuelve a encontrar estos URL envía esas *cookies* específicas al servidor web.
Existen diferentes tipos de *cookies*: pueden ser duraderas o, como es el caso de las denominadas *cookies* de sesión, tener una duración limitada.
Se puede hacer que el ordenador desactive las *cookies* o que avise al usuario antes de aceptar una.

Correo web

Sistemas de correo electrónico que utilizan páginas web como interfaz (por ejemplo, Yahoo, HotMail, etc.). Al *correo web* se puede acceder desde cualquier sitio y el usuario no necesita conectarse a un *proveedor de servicios de Internet* concreto como cuando utiliza una cuenta normal de correo electrónico.

Cortafuegos

Es un método para garantizar la seguridad de una red. Se puede implementar en un *encaminador* único que filtra los paquetes indeseados, o puede hacer uso de una combinación de tecnologías de *encaminadores* y ordenadores centrales. Los *cortafuegos* se utilizan a menudo para proporcionar a los usuarios un acceso seguro a Internet, así como para separar el servidor web público de una empresa de su red interna. También se usan para mantener seguros segmentos de la red interna; por ejemplo, para proteger una subred de búsqueda o contabilidad que podría ser accesible a usuarios internos indiscretos de otros departamentos.

Encaminador

Un *encaminador* es un dispositivo que proporciona rutas a las *redes TCP/IP*, lo que significa que la ruta TCP/IP es dinámica, y depende de los fallos o la sobrecarga de

ciertas rutas o vínculos. También se puede utilizar como un *cortafuegos* entre un organismo e Internet y garantiza que de un *proveedor de servicios de Internet* determinado sólo puedan proceder direcciones IP autorizadas.

Encriptación

Codificación de información y mensajes de forma que, en principio, no pueda leerlos nadie aparte del destinatario previsto, que dispone de la clave o contraseña. Existen dos tipos principales de sistemas de *encriptación*:
- El sistema simétrico o de clave privada, que utiliza una clave secreta compartida por el emisor y el destinatario de un mensaje. Su principal ventaja es la velocidad de tratamiento y su principal inconveniente es la dificultad de compartir claves seguras con un gran número de usuarios.
- El sistema asimétrico o de clave pública, que utiliza un par de claves, generadas de forma que, incluso sabiendo una de ellas, es prácticamente imposible adivinar la otra. Los mensajes encriptados con una de las claves se desencriptan con la otra. Una de las claves se hace pública y se usa para encriptar los mensajes que cada usuario desencripta con su clave privada secreta. La clave privada se usa también para firmar mensajes digitalmente.

Firma digital

Una *firma digital* es una cadena de datos que se añade a un mensaje y garantiza su *integridad* encriptándolo (o encriptando un resumen del mensaje) con la clave privada del firmante. Cualquiera que reciba el mensaje firmado puede comprobar si ha sido modificado simplemente desencriptando la firma con la clave pública del emisor y comparando la cadena desencriptada con el mensaje original o su resumen.

Firma electrónica

Datos electrónicos adjuntos o asociados lógicamente a otros datos electrónicos que sirven como método de *autentificación* (apartado 1 del artículo 2 de la Directiva sobre *firmas electrónicas*).

Hipervínculo

Un vínculo predefinido entre dos objetos. El vínculo se muestra como texto o como un icono. En las páginas web, un *hipervínculo* de texto se muestra como texto subrayado, normalmente en azul, mientras que un *hipervínculo* gráfico es una pequeña imagen.

Husmeo

Los programas de *husmeo* pueden leer todos los paquetes de datos de una red y presentar en texto claro toda comunicación no encriptada. La forma más sencilla de *husmeo* se puede realizar utilizando un ordenador personal normal conectado a una red, con programas que se pueden encontrar fácilmente.

Identificación de la línea de llamada (CLI)

Cuando se realiza una llamada, la CLI permite al usuario que la recibe identificar al usuario que lo llama mostrando el número de la línea de llamada.

Integridad de los datos

Proceso con el que se evita la destrucción o la adulteración accidental de una base de datos.

Java y JavaScript

Java es un lenguaje de programación que no puede ser utilizado por el programador ocasional, ni mucho menos por el usuario. *JavaScript* es un lenguaje de scripts que utiliza una sintaxis similar a *Java,* pero que no está compilado en un código de bytes. Permanece en código fuente incrustado en un documento HTML y el intérprete de *JavaScript* lo tiene que traducir línea por línea a código de máquina. El *JavaScript* está muy extendido y lo aceptan todos los navegadores de la Web. Su alcance es más limitado que el de *Java,* y principalmente se aplica a los elementos de la propia página.

Metaetiquetas

Las *metaetiquetas* son etiquetas HTML que proporcionan información sobre una página web. Al contrario que las etiquetas HTML normales, las *metaetiquetas* no afectan al modo en que se muestra la página, sino que dan información sobre su creador, la frecuencia de las actualizaciones, el tema que trata y las palabras clave que representan el contenido de la página. Muchos motores de búsqueda utilizan esta información al establecer sus índices.

Minería de datos

Implica "excavar toneladas de datos" para descubrir patrones y relaciones contenidos en la actividad y el pasado de la empresa. Normalmente se realiza con programas que analizan los datos automáticamente.

Módem

(**MO**dulador-**DEM**odulador) Aparato que adapta un terminal u ordenador a una línea de teléfono analógica convirtiendo cada señal digital en frecuencias de audio y viceversa. Normalmente, el término se refiere a *módems* de 56 kbps (V.90), la máxima velocidad actual, o a *módems* más antiguos de 28,8 kbps (V.34), aunque también se puede aplicar a *módems* de velocidad superior, a *módems* de línea de suscripción digital, o a adaptadores de terminal RDSI, todos ellos digitales y no *módems* técnicamente. Un *módem* es un convertidor analógico-digital y digital-analógico que también puede conectar con la línea, responder la llamada y controlar la velocidad de transmisión. Los *módems* han evolucionado de 300, 1 200, 2400, 9 600, 14 400, 28 800 y 33 300 a 56 000 bps. Cualquiera que sea su velocidad máxima, el *módem* siempre es capaz de funcionar a ciertas velocidades inferiores para poder acomodarse a *módems* más antiguos o adaptarse a una velocidad inferior en caso de líneas telefónicas de menor calidad.

OLAP

"**O**n**L**ine **A**nalytical **P**rocessing" (tratamiento analítico en línea). Software de apoyo para la toma de decisiones que permite al usuario analizar rápidamente información resumida en jerarquías y vistas multidimensionales. Por ejemplo, las herramientas de *OLAP* se utilizan para analizar tendencias de ventas e información financiera. Permiten que los usuarios exploren grandes cantidades de estadísticas para aislar los productos más volátiles. Los productos *OLAP* tradicionales, también conocidos como *OLAP* multidimensional o MOLAP, resumen transacciones en vistas multidimensionales preparadas de antemano. Las consultas de los usuarios a este tipo de bases de datos son extremadamente rápidas, pues la consolidación ya se ha realizado. El *OLAP* coloca los datos en una estructura cúbica que el usuario puede girar, lo que resulta especialmente indicado para análisis financieros.

Pancarta

Las *pancartas* publicitarias son pequeños cuadros gráficos que aparecen sobre el contenido del sitio web o están integrados en él.

Portal

Los *portales* proporcionan una vista general de los vínculos web de una manera ordenada. Pasando por un *portal*, el usuario de Internet puede visitar fácilmente otros sitios web seleccionados de otros proveedores de contenidos.
Los *portales* modernos son "supersitios" que ofrecen una serie de servicios tales como búsqueda en la Web, noticias, guías de páginas blancas y amarillas, correo electrónico gratuito, grupos de debate, compras en línea y vínculos con otros sitios.

Protocolo

En este contexto, un *protocolo* es una serie de normas técnicas que han de observar los dos participantes en un intercambio de información. Los *protocolos* están organizados en una jerarquía de lo que se denomina capas. Cada capa se encarga de manejar un aspecto particular del proceso de las telecomunicaciones y ofrece funciones básicas que utilizarán las capas superiores. Tradicionalmente, en Internet el *protocolo* TCP/IP se utiliza siempre como una capa intermedia. Ethernet (utilizado en redes locales), *ADSL* (usado en las líneas telefónicas), ATM (modo de transferencia asíncrona, usado por los operadores de telecomunicaciones), X-75 (usado en líneas RDSI) y PPP (*protocolo de punto a punto*, usado en líneas telefónicas normales) son ejemplos de *protocolos* de nivel inferior. En el otro extremo, HTTP (para navegar), SMTP (*protocolo* simple de transferencia de correo, para el correo electrónico), POP (*protocolo* de oficina de correo, también para el correo electrónico) y FTP (para transferir ficheros) son *protocolos* de nivel superior. Esto significa que cualquier amenaza potencial a la privacidad del *protocolo* TCP/IP será una de las debilidades de los *protocolos* superiores. Básicamente, las capas son una serie de subprogramas instalados en un ordenador conectado a Internet.

Protocolo de configuración dinámica del host (DHCP)

El *protocolo de configuración dinámica del host* (DHCP) es un *protocolo* de Internet para automatizar la configuración de los ordenadores que utilizan TCP/IP. El DHCP se puede utilizar para asignar automáticamente direcciones IP (http://www.dhcp.org).

Protocolo de punto a punto

El *protocolo de punto a punto* es un *protocolo* de telecomunicación muy utilizado para conectar dos ordenadores a través de su puerto serie o un *módem* conectado en él. Es el *protocolo* de capa inferior más usado entre el ordenador personal de un usuario privado y el servidor de acceso a Internet de un *proveedor de servicios de Internet* cuando se establece una conexión TCP/IP con líneas telefónicas clásicas.

Proveedor de servicios de Internet

Empresa que proporciona acceso y conexiones a Internet a particulares y empresas.
Los pequeños *proveedores de servicios de Internet* proporcionan el servicio mediante *módems* y RDSI, mientras que los mayores ofrecen también conexiones de línea privada. Generalmente, los consumidores pagan un precio fijo al mes, pero a éste se pueden sumar otros costes. Pagando una cuota se puede crear y mantener un sitio web en el servidor del *proveedor de servicios de Internet*, lo que permite a una organización pequeña estar presente en la Web con su propio nombre de dominio.
Los grandes *proveedores de servicios de Internet* también ofrecen bases de datos privadas, foros y otros servicios.
En este informe, el término *proveedor de servicios de Internet* incluye normalmente a los proveedores de acceso a Internet, término que únicamente se utiliza cuando es obvio que sólo se habla del acceso a Internet. En el resto de los casos se habla de *proveedor de servicios de Internet*.

Red TCP/IP

Las *redes TCP/IP* (*protocolo* de control de transporte/*protocolo* de Internet) se basan en la transmisión de paquetes pequeños de información, cada uno de los cuales contiene la dirección IP del emisor y del destinatario. Estas redes funcionan sin conexiones, lo que significa que, al contrario de lo que sucede con la red telefónica, por ejemplo, no es necesaria una conexión previa entre dos dispositivos para iniciar la comunicación. Esto permite igualmente mantener diversas comunicaciones con interlocutores distintos de forma simultánea.

Series de clics

Información derivada del comportamiento de un individuo, su recorrido o las elecciones que ha realizado durante su visita a un sitio web. Contienen los vínculos que un usuario ha seguido y están almacenados en el servidor web (el ordenador del *proveedor de servicios de Internet*, en el caso de los usuarios que no tengan un servidor web propio).

Servidor proxy

El *servidor proxy* es un servidor intermediario entre el usuario de Internet y la Red. Actúa como una *caché web* y mejora de una forma espectacular el funcionamiento de

Internet. Muchas grandes organizaciones o proveedores de acceso a Internet ya han aplicado esta solución. Cada página, imagen o logotipo descargado desde el exterior por un miembro de una organización se almacena en una caché en el *servidor proxy* y queda automáticamente disponible para los otros miembros de la misma organización.
Ya no es necesario que cada miembro de la organización situado antes del *servidor proxy* tenga su propia dirección IP, pues no accede directamente a Internet.

Sistema de nombres de dominio (DNS)

El DNS *(sistema de nombres de dominio)* es un mecanismo para asignar nombres a ordenadores identificados con una dirección IP. Estos nombres adoptan la forma <nombre>.dominio de nivel superior, donde <nombre> es una cadena formada por una o varias subcadenas separadas por un punto.

Software compartido

Software que se puede descargar de Internet. Normalmente, se puede descargar de forma gratuita para probarlo, pero para que su uso sea legal posteriormente se ha de pagar por él. Los programas que se pueden descargar y usar completamente gratis se conocen con el nombre *software gratuito.*

Terceros de confianza[221]

Un *tercero de confianza* se puede describir como una entidad a la que otras entidades confían sus actividades y servicios relacionados con la seguridad.
Un *tercero de confianza* ofrecerá servicios de valor añadido a los usuarios que deseen aumentar la seguridad y la confianza de los servicios que reciben y facilitar la realización de comunicaciones seguras con sus socios empresariales. Los *terceros de confianza* han de demostrar un alto nivel de *integridad*, confidencialidad y garantía en los resultados de los servicios y la información necesarios para las comunicaciones entre aplicaciones comerciales. Por otra parte, los usuarios requerirán los servicios de los *terceros de confianza* cuando los necesiten, en el marco de un contrato de prestación de servicios.
Normalmente, un *tercero de confianza* será una organización que ha obtenido una licencia o acreditación de una autoridad reguladora y que, partiendo de una base comercial, presta servicios de seguridad a una amplia gama de órganos, incluidos los de los sectores de las telecomunicaciones, las finanzas y el comercio minorista.
Por ejemplo, se podría recurrir a un *tercero de confianza* para garantizar la asignación de *firmas digitales* que garanticen la *integridad* de los documentos. Además, pueden ofrecer servicios de *encriptación* de extremo a extremo a los usuarios y proponer, por ejemplo, funciones de almacenamiento o recuperación de claves para recuperar ficheros en caso de pérdida de la clave de *encriptación* (normalmente, en caso de documentos o archivos encriptados por empleados) o como apoyo en peticiones de interceptación legal.
El recurso a *terceros de confianza* está sujeto fundamentalmente a la confianza que tengan en él las entidades a las que prestan servicios.

UMTS

[221] Definición tomada del ETSI (Instituto Europeo de Normas de Telecomunicaciones), *"Requirements for TTP services"*.

El *UMTS* (sistema universal de telecomunicaciones móviles) es un *protocolo* de banda ancha de "tercera generación" de transmisión en paquetes e inalámbrico, que ofrecerá una velocidad de transmisión superior a 2 Mbps. Este nuevo *protocolo* de banda ancha permitirá la transmisión de señales digitales de vídeo a aparatos portátiles con la misma calidad que en la televisión. Actualmente, la red GSM permite velocidades en torno a los 11 kbps, suficientes para transmitir señales sonoras pero no imágenes en movimiento[222].

WAP

El *WAP* (*protocolo* de aplicación inalámbrica) es un *protocolo* de telecomunicaciones diseñado entre diversos fabricantes de teléfonos móviles. Permite el acceso a servicios de Internet como el correo, la charla electrónica o la navegación por la Web, desde un teléfono móvil especializado[223].

Hecho en Bruselas, el 21 de noviembre de 2000

Por el Grupo de Trabajo

Stefano RODOTA

Presidente

[222] Véase http://www.umts-forum.org/.
[223] Para obtener más información, véase: http://www.wapforum.org.