COMISIÓN EUROPEA
DIRECCIÓN GENERAL XV
Mercado Interior y Servicios Financieros
Libre circulación de la información, Derecho de sociedades e información financiera
**Libre circulación de la información, protección de datos y sus aspectos internacionales**

XV D/5022/97 ES final
**WP 6**

**Grupo de Trabajo sobre protección de las personas en lo que respecta al tratamiento de datos personales**

# RECOMENDACIÓN 3/97

## Anonimato en Internet

Adoptada por el Grupo de Trabajo el 3 de diciembre de 1997

**EL GRUPO DE TRABAJO SOBRE LA PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES**,

creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

visto el artículo 29 y el apartado 3 del artículo 30 de la citada Directiva,

visto su Reglamento Interno y, en particular, los artículos 12 y 14 del mismo,

ha adoptado la siguiente Recomendación:

El Grupo de Trabajo, en su octava reunión, celebrada en Bruselas el 3 de diciembre de 1997, aprobó el documento de debate XV/5022 ("Anonimato en Internet") y tomó nota del Informe y Orientaciones elaborados por el Grupo de Trabajo Internacional sobre protección de datos en el ámbito de las telecomunicaciones ("Memorando de Budapest - Berlín sobre protección de datos e intimidad en Internet");

Recomienda que la Comisión Europea elabore propuestas basándose en el adjunto documento de debate ("Anonimato en Internet"; Anexo 1) y en las recomendaciones contenidas en el Memorando de Budapest - Berlín (Anexo 2), con objeto de apoyar su aplicación a través de las oportunas instancias internacionales.

1 DO L 281 de 23.11.1995, p. 31.

**Documento de debate - Anonimato en Internet**

**Aprobado en la octava reunión**

## Introducción

El rápido desarrollo de Internet y el importante incremento del número y tipos de servicios disponibles a través de este nuevo medio están abundantemente documentados. Es evidente que el fenómeno de Internet ya está operando una transformación en nuestra forma de vida y hábitos de trabajo como empleados y ciudadanos, introduciendo profundos cambios en las formas de adquisición y venta de bienes y servicios, y reconfigurando la actuación empresarial en los sectores público y privado.

Estos cambios tan espectaculares y de gran alcance llevan inevitablemente aparejados nuevos problemas y presentan nuevos retos a quienes tienen por misión definir y desarrollar normas de orden público y velar por su cumplimiento. En un principio, la atención de los responsables políticos se centró, sobre todo, en el potencial de Internet como foro de actividades delictivas o comportamientos indeseables "en línea" (como, por ejemplo, distribución de pornografía infantil) y como medio de comunicación "seguro" para facilitar acciones delictivas "fuera de línea".

A nivel europeo, fueron fundamentalmente esas posibilidades las que dieron pie a la adopción de una serie de iniciativas, a saber: Libro Verde sobre la protección de los menores y de la dignidad humana en los servicios audiovisuales y de información (COM(96) 483 final), Comunicación de la Comisión sobre contenidos ilícitos y nocivos en Internet (COM(96) 487), Resolución del Consejo, de 28 de noviembre de 1996, sobre contenidos ilícitos y nocivos, e Informe del Grupo de Trabajo sobre contenidos ilícitos y nocivos elaborado en la reunión informal del Consejo celebrada en Bolonia.

Gradualmente, sin embargo, se ha ido poniendo de manifiesto que el tema comporta otros muchos aspectos. La Comunicación de la Comisión "Iniciativa europea de comercio electrónico" (COM(97) 157) se propone ampliar el debate para hacerlo extensivo a otra serie de ámbitos importantes, tales como la fiscalidad (en particular el IVA) de la actividad comercial en línea y la protección de los derechos de propiedad intelectual en relación con contenidos distribuidos en línea.[2]

En todos estos ámbitos se están discutiendo nuevas ideas y proponiendo posibles soluciones tendentes a asegurar que los valores tradicionales y los intereses sociales desarrollados a lo largo de decenios se sigan manteniendo en esta nueva era tecnólogica. Un problema común a muchos de estos ámbitos es la dificultad de detectar actividades ilícitas que puedan haberse llevado a cabo y de identificar posteriormente a la persona responsable. ¿Quién ha introducido en Internet una determinada muestra de pornografía infantil? ¿Quién ha cargado en su ordenador una determinada obra protegida por derechos

[2] Este último tema se ha tratado ya en un Libro Verde y en la Comunicación de la Comisión "Seguimiento del Libro Verde sobre los derechos de autor y los derechos afines en la Sociedad de la Información".

de autor? ¿Quién ha omitido declarar el IVA correspondiente a servicios ofrecidos en línea?

Una reacción lógica ante este tipo de problemas ha sido la propuesta de que toda persona que desee tener acceso a Internet y a sus diversos servicios en línea se identifique debidamente, y de que sea posible localizar toda actividad realizada en línea.

**El problema de la intimidad**

El desarrollo de normas con respecto a Internet no se produce en el vacío, sino en el contexto de principios y valores bien establecidos. Quienes critican los intentos de restringir o regular la actividad en el ciberespacio suelen invocar el derecho a la libertad de expresión, derecho fundamental garantizado en Europa por el artículo 10 del Convenio Europeo de los Derechos Humanos (CEDH) e incorporado como principio general del Derecho comunitario por el apartado 2 del artículo F del Tratado de la Unión Europea. Sin embargo, el derecho a la intimidad (artículo 8 del CEDH, incorporado igualmente al Derecho comunitario) es asimismo importante a la hora de evaluar cualquier norma con respecto a Internet.

A lo largo de los últimos 25 años, se ha ido haciendo patente que una de las mayores amenazas que pesan sobre el derecho fundamental a la intimidad es la capacidad que tienen algunas organizaciones de acumular gran cantidad de información sobre los particulares, en forma digital, que permite su manipulación, alteración y transmisión a terceros con enorme rapidez (y actualmente a un coste muy bajo). La inquietud que suscita esta evolución y la posibilidad de que se haga uso indebido de tales datos personales ha llevado a todos los Estados miembros de la UE (y ahora a la Comunidad, con la Directiva 95/46/CE) a adoptar disposiciones específicas sobre protección de datos en las que se establece un marco normativo que regula el tratamiento de la información de carácter personal.

Uno de los principios fundamentales de la protección de datos (veánse la letra c) del apartado 1 del artículo 6 y el artículo 7 de la Directiva 95/46/CE) es que los datos personales obtenidos en cualquier situación deberán limitarse a lo que resulte necesario y pertinente para el propósito que se persigue. Toda información de carácter personal constituye potencialmente una amenaza para la intimidad de la persona, por lo que debe garantizarse que la información que se obtenga en cualquier circunstancia esté destinada a fines legítimos y que la cantidad de información obtenida se limite al mínimo.

Una característica de las redes de telecomunicaciones, y de Internet en particular, es su capacidad de generar una ingente cantidad de datos transaccionales (datos generados a fin de asegurar conexiones correctas). La posibilidad de utilizar las redes de modo interactivo (característica específica de numerosos servicios de Internet) hace aumentar aún más la cantidad de datos transaccionales. Así, al consultar un periódico en línea, el usuario "interacciona" seleccionando las páginas que desea leer, y tal selección crea un "flujo" ("*clickstream*") de datos transaccionales. En cambio, los servicios informativos más tradicionales se utilizan de forma mucho más pasiva (la televisión, por ejemplo), limitándose la interactividad al ámbito no automatizado de los kioskos y las bibliotecas. Aun cuando en algunos ordenamientos los datos transaccionales pueden disfrutar de algún

grado de protección en virtud de las normas que protegen la confidencialidad de la correspondencia, el incremento masivo de dichos datos suscita legítima inquietud.

A medida que evolucionen los servicios en línea, aumentando su complejidad y su popularidad, irá adquiriendo más importancia el problema de los datos transaccionales. A dondequiera que se accede en Internet, se deja un rastro digital, de manera que, al ser cada vez mayor el número de actividades de nuestro quehacer cotidiano que se realizan en línea, irá aumentando la información que sobre nuestras ocupaciones, gustos y preferencias quede registrada.

Con todo, la amenaza a nuestra intimidad no se deriva únicamente de la existencia de gran cantidad de datos personales en Internet, sino también del desarrollo de soportes lógicos capaces de buscar en la red y recopilar todos los datos disponibles sobre una persona determinada. Un artículo reciente del *Minneapolis Star Tribune* explicaba cómo puede elaborarse una biografía pormenorizada de una persona seleccionada al azar sirviéndose de dichos soportes lógicos y extrayendo información de todos los grupos de debate en los que aquélla haya participado. El periódico pudo obtener la dirección y el número de teléfono de la persona seleccionada, y descubrir dónde nació, dónde realizó sus estudios, su profesión, su actual lugar de trabajo, su interés por el teatro de aficionados, su tipo de cerveza favorita, sus preferencias en materia de restaurantes y de lugares de vacaciones, y sus opiniones acerca de temas tan dispares como Bill Gates o el estado “socialmente represivo” de Indiana. En los Estados Unidos existen ya una serie de emplazamientos de Internet donde se comercializan estos “servicios de búsqueda”.

**Datos anónimos: una manera de solventar el problema de la intimidad**

Los datos transaccionales sólo suponen una amenaza a la intimidad de las personas si se refieren a alguien a quien puede identificarse. Es evidente, por tanto, que una manera de conjurar esta amenaza consistiría en cerciorarse de que, siempre que sea viable, los rastros creados al utilizar Internet no permitan identificar al usuario. De garantizarse el anonimato, cualquiera podrá participar en la revolución de Internet sin temor a que queden registrados todos sus movimientos y a que se acumule información sobre su persona que pueda utilizarse más adelante con fines contrarios a su voluntad.

La pretensión de anonimato en las comunicaciones en línea se considera ya plenamente legítima en determinadas situaciones, como, por ejemplo, cuando una persona que es víctima de un delito sexual o padece una dependencia como las drogas o el alcohol quiere compartir sus experiencias con otras, cuando una persona que contempla la posibilidad del suicidio busca ayuda especializada en línea, o cuando una persona pretende denunciar un delito sin riesgo de represalias. En otros casos, la garantía de anonimato sirve para reforzar no sólo la intimidad, sino asimismo la libertad de expresión, como cuando disidentes políticos de un país sometido a un régimen totalitario desean poner de manifiesto su oposición a dicho régimen y llamar la atención sobre la violación de los derechos humanos.

Sin embargo, la necesidad de anonimato no se limita a estos casos específicos. En efecto, por su mera existencia, 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.

## Conciliar la intimidad con otros objetivos de orden público

Es evidente, pues, que los gobiernos y las organizaciones internacionales se enfrentan a una disyuntiva al tratar el problema del anonimato en Internet. Por una parte, la posibilidad de mantener el anonimato resulta esencial para el respeto de los derechos fundamentales a la intimidad y a la libertad de expresión en el ciberespacio. Por otra, la posibilidad de participación y de comunicación en línea sin revelar la propia identidad se contrapone a las iniciativas que se están desarrollando en apoyo de otros objetivos fundamentales de orden público, como la lucha contra los contenidos ilícitos y nocivos, contra el fraude financiero y contra las infracciones en materia de derechos de autor.

Por supuesto, esta aparente contraposición entre distintos objetivos de orden público no es nueva y, como subraya el Libro Verde de la Comisión sobre la protección de menores y la dignidad humana en los servicios audiovisuales y de información, el Convenio Europeo de Derechos Humanos ya establece un marco para la resolución de tales conflictos, a saber, un conjunto de derechos fundamentales sujetos a determinadas restricciones por motivos específicos, entre ellos la prevención de la delincuencia. En relación con tales restricciones, el Tribunal Europeo de Derechos Humanos ha desarrollado en su jurisprudencia el *principio de proporcionalidad* como criterio esencial de la conformidad de toda medida restrictiva aplicada a los derechos fundamentales garantizados por el Convenio.

El hecho de que se haya desarrollado tal jurisprudencia demuestra que siempre ha sido necesario encontrar un equilibrio entre objetivos contrapuestos de orden público. En el contexto de los medios de comunicación fuera de línea más tradicionales, como los envíos postales (cartas o paquetes), el teléfono, los periódicos o las transmisiones por radio y televisión, se ha logrado un equilibrio entre los citados objetivos. Los responsables políticos se enfrentan actualmente al reto de asegurar que este planteamiento equilibrado, que garantiza los derechos fundamentales, permitiendo al mismo tiempo restricciones proporcionadas de los mismos en circunstancias limitadas y específicas, se mantenga en el nuevo contexto del ciberespacio. Piezas esenciales de este equilibrio serán la posibilidad de participar en la comunicación en línea de forma anónima y los límites de tal participación.

## Aprender del pasado para encontrar soluciones de cara al futuro

Existe un claro consenso en cuanto a la imposibilidad de eximir la actividad desarrollada a través de Internet de los principios jurídicos fundamentales aplicados en otros ámbitos. Internet no es un gueto anárquico donde no se aplican las normas por las que se rige la sociedad. Análogamente, no obstante, la capacidad de los gobiernos y Administraciones públicas para restringir los derechos de las personas y controlar las actuaciones potencialmente ilícitas no debería ser mayor en Internet que en el mundo exterior, no automatizado. La exigencia de que las restricciones de los derechos y libertades fundamentales estén debidamente justificadas y sean necesarias y proporcionadas a otros objetivos de orden público debe cumplirse también en el ciberespacio.

El principio conforme al cual el régimen aplicable a Internet no debe ser más o menos favorable que el aplicable a tecnologías más antiguas está recogido tanto en la introducción a la Comunicación de la Comisión sobre contenidos ilícitos y nocivos en Internet, donde se afirma que "lo que es ilícito fuera de línea lo es también en línea", como en el Informe del Grupo de Trabajo sobre contenidos ilícitos y nocivos en Internet, que en su segunda propuesta de acción futura establece el principio de que "deberá otorgarse el mismo grado de libertad de circulación a la información que se transmite por Internet que a la que se difunde en papel".

El problema del anonimato debería tratarse con arreglo al mismo planteamiento. Tal como se afirma, con razón, en la "Declaración Ministerial de Bonn"[3], debería seguirse la máxima según la cual si el usuario puede mantener el anonimato fuera de línea, deberá ofrecérsele la misma posibilidad en línea. Habrán de examinarse los distintos servicios y actividades disponibles en Internet y, en lo posible, establecer analogías con los servicios existentes basados en modos de comunicación y formas de entrega más tradicionales. Tales comparaciones aportarán información valiosa sobre los ámbitos en que resulta oportuno ofrecer la posibilidad de mantener el anonimato y aquéllos en que no es aconsejable tal posibilidad.

**Correo electrónico (correspondencia de punto a punto a través de Internet)**

Actualmente, la mayor parte de las comunicaciones de correo electrónico identifican al emisor ya sea a través de su propia dirección electrónica o a través de la dirección Internet (IP). Dicha información suele estar al alcance tanto del destinatario del mensaje como de los proveedores de acceso y de servicios que intervienen en la operación. Hay, con todo, dos tipos de mecanismos alternativos que permiten mantener el anonimato en cierta medida:

*1)* *servicios de reexpedición anónima*: el proveedor de acceso puede ofrecer esta opción, o bien pueden dirigirse los mensajes a un servicio específico que garantiza el anonimato, que los reexpide de forma anónima;

*2)* *acceso anónimo a la red*: puede accederse a Internet de forma anónima, pagando por adelantado, por ejemplo, por un tiempo determinado de utilización y recibiendo una dirección anónima de correo electrónico, o a través de un kiosko público de Internet.

Los servicios de reexpedición anónima implican el mantenimiento de un nexo entre el remitente del mensaje y el propio mensaje, nexo que puede ser reconstruido con posterioridad, por ejemplo, con motivo de una investigación policial. Así pues, no garantiza el anonimato del mismo modo que la segunda alternativa y es preciso que esté regulada la utilización que hace el servicio de los datos de identificación que conserva. No obstante, ambas posibilidades comportan importantes ventajas desde la óptica de la intimidad de las personas, por lo que deben mantenerse y fomentarse.

---

[3] Declaración Ministerial de la Conferencia Ministerial sobre Redes mundiales de información, celebrada en Bonn los días 6 a 8 de julio de 1997.

La existencia de una posibilidad de anonimato en el correo electrónico reviste particular importancia frente a otras teconologías tradicionales de comunicación de punto a punto. Así, por ejemplo, el anticuado servicio de correos es mucho más respetuoso de la intimidad, ya que puede enviarse una carta normal sin revelar la propia identidad. El proveedor de servicios postales no puede obtener dato transaccional alguno que permita la identificación del remitente de la comunicación (a menos que éste decida facilitar sus datos en el exterior del sobre). Asimismo, el sistema de pago más extendido (el sello de correos) es totalmente anónimo. Más aún, el remitente puede no darse a conocer siquiera al destinatario de la carta.

También los sistemas tradicionales de telefonía ofrecen un mayor grado de anonimato que el correo electrónico. La amplia disponibilidad de cabinas públicas permite acceder a la red de forma anónima y los servicios pueden pagarse en efectivo o mediante tarjetas prepagadas anónimas, de manera que las llamadas efectuadas por este sistema no crean datos transaccionales identificables. Con todo, se crean datos transaccionales cuando un abonado efectúa una llamada desde su teléfono particular, y ha sido preciso introducir normas de protección de datos (que están siendo actualmente armonizadas a nivel comunitario a raíz de la Directiva "RDSI"[4]) con objeto de limitar el plazo de conservación de dichos datos y los fines para los que pueden utilizarse. No obstante, el autor de la llamada permanece anónimo para el destinatario de la misma en tanto éste no descuelgue el teléfono, a menos que esté instalado un dispositivo de identificación de la línea llamante (CLI), que permite al destinatario ver el número de su interlocutor antes de contestar la llamada. Sin embargo, tal es la incidencia de la CLI en la intimidad de los autores y los destinatarios de llamadas telefónicas, que se ha considerado necesario incluir un artículo específico en la Directiva antes citada tendente a ofrecer a las personas la posibilidad de impedir la transmisión de su número si lo desean. Esta disposición constituye un precedente a tener en cuenta en el contexto de la correspondencia en línea de punto a punto.

Pueden darse casos en que estén justificadas las restricciones impuestas a las comunicaciones anónimas por correo electrónico, por ejemplo, si hay indicios de que una comunicación determinada guarda relación con la preparación de un acto terrorista o de algún otro delito grave. Tales restricciones pueden llevar a exigir a un reexpedidor anónimo que desvele a la policía la verdadera identidad de las partes que intervienen en una comunicación. No obstante, toda restricción deberá respetar el criterio de proporcionalidad y aplicarse atendiendo estrictamente a las características de cada caso.

**Grupos de debate, tablones de anuncios y otros foros públicos de debate**

La comunicación a través de Internet no siempre adopta la forma de correspondencia privada de punto a punto. Los "grupos de debate" ("*newsgroups*") y las "salas de charla" ("*chat rooms*"), dedicados a temas concretos o a intereses compartidos son numerosos y gozan de gran popularidad. Las personas que aportan material para los mismos lo hacen a sabiendas de que dicho material va a estar al alcance de un sector amplio del público,

4 Directiva 97/66/CE 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 telecomunicaciones, aprobada, pero pendiente aún de publicación.

entre el que pueden incluirse niños u otras personas vulnerables. Así las cosas, suscita legítima inquietud la naturaleza de las contribuciones y es indispensable cerciorarse de que no se difundan contenidos inadecuados en foros de tan fácil acceso y/o de que puedan atribuirse responsabilidades si los contenidos difundidos resultan ser ilícitos.

Existen distintas posibilidades para ejercer cierto control sobre los citados "grupos de debate". Una de ellas es que pueda identificarse a las personas que hacen aportaciones y que se conserve un rastro de datos cada vez que se recibe una contribución. Cabe preguntarse, sin embargo, si esta solución es proporcionada al problema y si es realmente viable. Al fin y al cabo, en el mundo no virtual hay numerosos tablones de anuncios -en locales de oficinas, escuelas y universidades- en los que se invita a la gente a exponer información. Sería inconcebible que se controlara de la misma manera el acceso a dichos tablones de anuncios.

Sin embargo, hay otras posibilidades. Así, por ejemplo, pueden desarrollarse soluciones contractuales para garantizar un cierto grado de "calidad de los contenidos". Alternativamente, el proveedor del servicio del grupo de debate podría asegurar en todo momento la intervención de un "moderador" cuya función consistiría en supervisar las contribuciones a fin de detectar posibles contenidos ilícitos y nocivos. Estos moderadores podrían cerciorarse de que los contenidos inadecuados se eliminaran con rapidez y de que se desconectara del grupo a aquellas personas que estuvieran en vías de hacer tales contribuciones. Las líneas telefónicas "de charla" ("*chat lines*") y "compartidas" ("*party lines*") han venido utilizando ese tipo de mecanismos para moderar la actuación de los participantes. Cabe incluso la posibilidad de atribuir al proveedor del servicio algún grado de responsabilidad jurídica por el material que difunde, de manera que aquél tenga interés en comprobar previamente todo el material que se recibe y publicar únicamente aquello que se considere lícito y aceptable para el consumo público. En tal supuesto, puede mantenerse el anonimato de los colaboradores, mientras que el proveedor del servicio asume una función semejante a la del editor de las cartas al director de un periódico.

Es éste un ámbito, además, en el que tal vez la tecnología pudiera aportar soluciones. Aun en el caso de que se considerase problemática la posibilidad de acceder de forma anónima a ciertos foros públicos, podría permitirse el acceso a las personas mediante la atribución de una "pseudoidentidad" por un proveedor de servicio especializado semejante al reexpedidor mencionado anteriormente. En tales casos, aunque en general se respetaría el anonimato, de existir indicios de actividades delictivas podría reconstruirse un nexo con la verdadera identidad del usuario considerado.

Es evidente, pues, que las colaboraciones totalmente anónimas a los foros de debate público plantean dificultades que no presentan las simples comunicaciones de punto a punto, y que deben desarrollarse mecanismos adecuados para impedir el uso indebido de dichos foros. Con todo, los derechos fundamentales a la intimidad y a la libertad de expresión no deben restringirse de manera desproporcionada mediante sistemas de identificación obligatoria, especialmente teniendo en cuenta la posibilidad de recurrir a medios más proporcionados de controlar y moderar los contenidos.

**Navegación pasiva por emplazamientos Internet de la World Wide Web**

La mayor parte de los emplazamientos de la actual World Wide Web están destinados fundamentalmente a suministrar información al público en general, y millones de personas dedican el tiempo que pasan en línea a navegar ociosamente por los innumerables emplazamientos a los que se puede acceder.

Lo más parecido a esta actividad en el mundo no virtual sería el hojear libros en bibliotecas públicas o librerías, o el pasear por las calles mirando escaparates. Al igual que en el caso de la navegación en línea, a menudo no se tiene intención alguna de comprar, sino simplemente la curiosidad de comprobar qué se puede obtener. Hay, no obstante, una diferencia fundamental y es que hojear libros en una biblioteca o pasear mirando escaparates puede hacerse de forma casi por completo anónima, en tanto que navegar en la Web deja sistemáticamente un registro digital permanente e identificable.

No hay motivo alguno de orden público o interés general para que dichos rastros sean identificables, salvo el posible deseo del usuario de que lo sean. Por supuesto, la obtención de los nombres y direcciones de correo electrónico de los visitantes de un emplazamiento comercial en la Web resultarán de utilidad para su propietario, que podrá utilizarlos con fines comerciales. Sin embargo, la obtención de tales datos en relación con personas que se limiten a navegar por la red deberá realizarse de forma totalmente transparente y con el consentimiento consciente del usuario. Por su parte, quienes deseen navegar en la World Wide Web manteniendo el anonimato deberán poder hacerlo con entera libertad.

**Adquisición de bienes y servicios a través de Internet**

A medida que se desarrollen medios de pago seguros, junto con mecanismos que garanticen la integridad de los datos y la validación de las transacciones (p. ej., firmas digitales), Internet irá adquiriendo preeminencia como espacio de actividad comercial al que los particulares acuden no sólo en busca de información, sino también para adquirir bienes y servicios. En este sentido, el interrogante que debe despejarse es si para comprar a través de Internet las personas han de ser identificables, o si debería ofrecérseles la posibilidad de mantener el anonimato.

En el mundo no virtual suelen efectuarse pagos en efectivo de manera anónima, lo que es más, se considera que ésa es la forma más cómoda y eficiente de pagar por bienes y servicios, en particular por los que comportan desembolsos de escasa cuantía. Al vendedor de un pequeño local comercial no le interesa la identidad de su cliente, sino tan sólo que el dinero que se le entregue sea moneda de curso legal.

Cuando se trata de compras de mayor entidad, los pagos en efectivo a menudo suponen complicaciones tanto para el comprador como para el vendedor. En efecto, los billetes de banco ocupan mucho espacio en las carteras y en las cajas registradoras y resulta arriesgado, por lo demás, guardar cantidades importantes de dinero. Por estos motivos, cuando el importe de la compra es elevado, suelen preferirse medios de pago no anónimos, como los cheques o las tarjetas de débito.

Como es natural, cuando se efectúa un pago mediante un crédito, deja de ser posible mantener el anonimato, ya que al comprar a crédito el particular contrae una deuda de la que ha de responder, por lo que debe dejarse constancia documental del vínculo entre la persona y la deuda contraída por la misma. En caso de que se utilice una tarjeta de

crédito, el particular deberá responder de su deuda ante el emisor de la tarjeta y no directamente ante el vendedor; será preciso, no obstante, que quede un rastro identificable de la transacción.

El comercio electrónico a través de Internet debería, en principio, ajustarse al modelo establecido para los pagos fuera de línea. Debería ofrecerse a los particulares la posibilidad de elegir entre distintos medios de pago seguros, incluido alguno que permitiera mantener el anonimato. A fin de hacer su utilización más atractiva, el dinero electrónico anónimo debería incluso presentar alguna ventaja destacable frente al dinero tradicional. En primer lugar, se podría, por ejemplo, permitir mantener una cantidad ilimitada de dinero en una pequeña tarjeta. En segundo lugar y sin que ello afectase a su carácter anónimo, la tarjeta podría llevar incorporados dispositivos de seguridad, como, por ejemplo, un código de acceso individual que únicamente conociera el usuario, lo que reduciría enormemente los riesgos en caso de pérdida. Estas características podrían hacer que el dinero electrónico anónimo resultara una opción interesante incluso para compras en línea de elevada cuantía.

Un requisito esencial que debería cumplir el dinero electrónico del tipo señalado sería la posibilidad de verificar su carácter "real", lo que implicaría la inclusión de características técnicas que impidieran su falsificación y garantizaran su autenticidad, sin que ello afectase a la posibilidad de utilizarlo de forma anónima.

Hay, no obstante, otras consideraciones de orden público que deben tenerse en cuenta a la hora de determinar la conveniencia de crear medios de pago anónimos en línea. La más importante es la lucha contra el blanqueo de capitales. En efecto, el blanqueo de grandes cantidades de dinero fruto de actividades delictivas -de las que el tráfico de drogas es la más frecuente-, ya sea amparándose en el anonimato u ocultándose tras una identidad ficticia, constituye un grave problema. A fin de impedir tal actividad, en 1991 se adoptó una Directiva (91/308/CEE) orientada a prevenir la utilización del sistema financiero para el blanqueo de capitales. Las principales disposiciones de esta Directiva obligan a las entidades de crédito y financieras a exigir la identificación de sus clientes antes de establecer cualquier relación comercial con los mismos y a conservar un registro de las transacciones durante un período de cinco años como mínimo.

No obstante, la Directiva no es, en sí, incompatible con los pagos anónimos, ya que se centra primordialmente en las transacciones con bancos y otras entidades de crédito y financieras[5], en tanto que los sistemas de dinero electrónico anónimo se utilizarían, sobre todo, en las transacciones entre particulares y comerciantes que no forman parte del sistema financiero. Sería lógico que se exigiera la identificación de las personas para retirar dinero electrónico de un banco, y tal vez para depositar importes elevados de dinero electrónico. Sin embargo, una vez que el dinero estuviera en su poder, no hay motivo alguno por el que no debiera ser anónimo, al igual que el dinero tradicional. En consecuencia, las necesidades de la policía y de las autoridades responsables del cumplimiento de la ley, cuya misión consiste en identificar a los culpables de operaciones de blanqueo de dinero, deberán contrapesarse cuidadosamente con las ventajas que para la

[5] Lo dispuesto en el artículo 12 puede llevar a ampliar el ámbito de aplicación de la Directiva de manera que incluya sectores tales como casinos y comerciantes en objetos de valor (arte, antigüedades, bienes inmuebles y metales preciosos).

intimidad de las personas representan los pagos anónimos. Si han de ponerse límites a la utilización de medios de pago anónimos, deberá ser únicamente cuando haya indicios claros de que el anonimato en una transacción dificulta realmente la detección del blanqueo de dinero. No parece que las transacciones de pequeño importe planteen problemas a este respecto, y es dudoso que incluso las operaciones de mayor entidad (p. ej., la adquisición en línea de soportes lógicos de un precio elevado) se utilicen para blanquear fondos.

## RESUMEN DE LAS PRINCIPALES CONCLUSIONES

- La posibilidad de mantener el anonimato es fundamental para que la intimidad de las personas goce de la misma protección en línea que fuera de línea.

- La posibilidad de anonimato no siempre resulta oportuna. A la hora de determinar en qué circunstancias lo es y en cuáles no, deben contrapesarse cuidadosamente los derechos fundamentales a la intimidad y a la libertad de expresión con otros objetivos importantes de orden público, entre ellos la prevención de la delincuencia. Las restricciones legales que puedan imponer los Gobiernos al derecho de mantener el anonimato o a los medios técnicos utilizados al efecto (p. ej., disponibilidad de productos de codificación) deberán en todo momento ser proporcionadas y limitarse a lo estrictamente necesario para proteger un interés general específico en una sociedad democrática.

- En la medida de lo posible, el equilibrio alcanzado en relación con tecnologías anteriores deberá preservarse en lo que respecta a los servicios ofrecidos a través de Internet.

- Deberá ser posible mantener el anonimato a la hora de enviar correo electrónico, navegar pasivamente por emplazamientos de la World Wide Web y adquirir la mayor parte de bienes y servicios a través de Internet.

- Aun cuando sean necesarios ciertos controles de los particulares que envían colaboraciones a los foros públicos en línea (grupos de debate, etc.), la exigencia de identificación de las personas resulta a menudo desproporcionada e inviable, por lo que debería optarse por otras soluciones.

- Los medios anónimos de acceso a Internet (p. ej., kioskos públicos Internet, tarjetas de acceso prepagadas) y los medios anónimos de pago constituyen dos elementos esenciales con vistas al verdadero anonimato en línea.

## Llevar a la práctica las conclusiones: recomendaciones operativas

Las anteriores conclusiones, que se refieren fundamentalmente al alcance del derecho legítimo de los particualres al anonimato en el contexto de Internet, describen la situación que ha de crearse para no ocasionar merma a la intimidad de las personas. No obstante, la situación actual es muy distinta, ya que el acceso de los usuarios a Internet y su actividad en la red raramente son anónimos. Los intentos de ofrecer servicios semianónimos (p. ej.,

reexpedidores anónimos) se han topado con problemas legales; la configuración técnica de los protocolos de Internet no permite fácilmente mantener el anonimato; y el medio de pago en línea más extendido sigue siendo la tarjeta de crédito, mientras que los experimentos con dinero electrónico anónimo no han hecho aún su irrupción en el mercado eletrónico general.

Para que la situación cambie, será preciso encontrar la manera de llevar a la práctica las conclusiones anteriormente enunciadas, lo que requerirá tomar medidas en distintas vertientes, a saber:

**1) Contexto normativo**

- El principio según el cual la obtención de datos personales de identificación deberá limitarse al mínimo necesario habrá de reconocerse en las normas nacionales e internacionales que se vayan desarrollando con vistas a regular Internet. Asimismo, dicho principio deberá incorporarse a los códigos de conducta, las directrices y demás instrumentos reguladores no legislativos que se elaboren. En su caso, deberá preverse el derecho de las personas a mantener, si lo desean, el anonimato.

**2) Contexto tecnológico**

- Habrán de intensificarse los debates en el consorcio de la World Wide Web con vistas a desarrollar una infraestructura y unos protocolos de Internet que favorezcan la actividad de los usuarios al amparo del anonimato.

- Los fondos destinados a investigación y desarrollo (como los disponibles en virtud del Quinto Programa Marco de Investigación y Desarrollo Tecnológico comunitario) deberán dirigirse específicamente a proyectos orientados a desarrollar medios de pago anónimos a través de Internet y medios de acceso anónimos (p. ej., terminales públicos de Internet).

**3) Contexto económico**

- Las Administraciones deberán estudiar la manera de ofrecer apoyo económico que impulse la adopción generalizada en el mercado de tecnologías que favorezcan la intimidad y permitan a las personas mantener el anonimato. Así, por ejemplo, podrían valerse de la influencia que les permite ejercer en el mercado el hecho de ser clientes importantes en materia de productos y servicios de TI para incluir, entre las condiciones de sus ofertas públicas, requisitos relativos al respeto de la intimidad. También podría estudiarse la posibilidad de favorecer los productos y servicios respetuosos de la intimidad por medio de subvenciones o desgravaciones fiscales, al igual que ocurre con los productos favorables al medio ambiente, como la gasolina sin plomo.

## 4) Sensibilización de los usuarios de Internet, los proveedores de acceso y servicios y el sector de la TI

- La mayoría de los usuarios de Internet no son conscientes de los riesgos que sus actividades en línea comportan para su intimidad. A este respecto, urge ofrecer consejo y orientaciones, tarea en la que deben desempeñar un papel importante las autoridades responsables de la protección de datos en todos los países. Las directrices elaboradas por la Comisión Española de Protección de Datos constituyen un ejemplo a seguir. Habrá que estudiar ahora la manera de dar la máxima difusión a tales directrices en la comunidad Internet.

- Análogamente, será necesario sensibilizar a todos aquellos que obtienen y procesan datos a través de Internet (proveedores de acceso y de servicios, emplazamientos de la Web) sobre las normas que les son aplicables en materia de protección de datos, que exigen, entre otras cosas, transparencia en la recogida de los mismos, y restringen los fines para los que pueden utilizarse y desvelarse los datos personales.