EN TORNO A LA CONSIDERACIÓN JURÍDICA DEL NÚMERO IP.

Ricard Martínez Martínez
Técnico de control de bases de datos
Universitat de València

sumario

resumen

El conocido como número IP juega un papel fundamental en la identificación de los ordenadores conectados en red. Internet funciona gracias al protocolo TCP/IP. El desarrollo de redes locales en los años 70 y 80 del siglo pasado obligaba a resolver distintos problemas. El más básico era, obviamente, establecer un método que permitiese generar la propia existencia de la red y junto a el máquinas capaces de dirigir la información identificando con plena certeza al emisor, al receptor y, por supuesto el mensaje. Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos. Dependiendo del su ámbito existen redes de área local "LAN" que, como su nombre indica, abarcan un espacio físico reducido como un edificio, un polígono, un campus universitario. Junto a ellas se citan las redes de área más extensa que abarcan regiones e incluso uno o más países, las "WAN". Finalmente las redes se interconectan entre si dando lugar a redes globales, en este sentido internet es una red de redes. Para poder interconectar los ordenadores en el mundo de las redes se requerían protocolos. Estos son normas o reglas necesarias para establecer la comunicación entre los nodos de una red. Los protocolos usados por todas las redes que forman parte de Internet se llaman abreviadamente TCP/IP. El protocolo TCP se orienta a regir la transmisión y requiere del Internet Protocol o IP.En las redes se denomina como host a cualquier ordenador conectado a la red, que disponga de un número IP que presta algún servicio a otro ordenador. Así el ordenador del usuario se denomina local host. Con este el usuario comienza su sesión de trabajo entrando en la red. Una vez en ella conecta con otras máquinas, ordenadores remotos (remote host) situados físicamente en cualquier parte del planeta. Para que esta comunicación se establezca se requiere que los dos ordenadores se identifiquen mediante una dirección llamada dirección IP o número IP. Cada ordenador puede tener una o varias IP que serán exclusivas y podrán ser asignadas con carácter estable, estáticas, o en cada sesión, IP dinámicas. Los IP son números de 32 bits representados habitualmente en formato decimal. Constan de cuatro valores en los que los dos primeros corresponden al número de red y los dos segundos al de la interfaz de red. Por otra parte los ordenadores también se denomina por referencia a los nombres de dominio. Así, dentro del dominio de la Universitat de València (http://www.uv.es/), una máquina que se denominase pc1 se identificaría por el nombre pc1.uv.es. Estos nombres también son exclusivos, no pueden existir dos máquinas con idéntico nombre.

1 ■ INTRODUCCIÓN

El conocido como número IP juega un papel fundamental en la identificación de los ordenadores conectados en red. Internet funciona gracias al protocolo TCP/IP. El desarrollo de redes locales en los años 70 y 80 del siglo pasado obligaba a resolver distintos problemas. El más básico era, obviamente, establecer un método que permitiese generar la propia existencia de la red y junto a el máquinas capaces de dirigir la información identificando con plena certeza al emisor, al receptor y, por supuesto el mensaje.

Una red es un conjunto de ordenadores conectados entre sí, que pueden comunicarse compartiendo datos. Dependiendo del su ámbito existen redes de área local "LAN[1]" que, como su nombre indica, abarcan un espacio físico reducido como un edificio, un polígono, un campus universitario. Junto a ellas se citan las redes de área más extensa que abarcan regiones e incluso uno o más países, las "WAN[2]". Finalmente las redes se interconectan entre si dando lugar a redes globales, en este sentido internet es una red de redes.

Para poder interconectar los ordenadores en el mundo de las redes se requerían protocolos. Estos son normas o reglas[3] necesarias para establecer la comunicación entre los nodos de una red. Los protocolos usados por todas las redes que forman parte de Internet se llaman abreviadamente TCP/IP. El protocolo TCP[4] se orienta a regir la transmisión y requiere del Internet Protocol o IP.

En las redes se denomina como host a cualquier ordenador conectado a la red, que disponga de un número IP que presta algún servicio a otro ordenador. Así el ordenador del usuario se denomina local host. Con este el usuario comienza su sesión de trabajo

NOTAS

entrando en la red. Una vez en ella conecta con otras máquinas, ordenadores remotos (remote host) situados físicamente en cualquier parte del planeta. Para que esta comunicación se establezca se requiere que los dos ordenadores se identifiquen mediante una dirección llamada dirección IP o número IP. Cada ordenador puede tener una o varias IP que serán exclusivas y podrán ser asignadas con carácter estable, estáticas, o en cada sesión, IP dinámicas. Los IP son números de 32 bits representados habitualmente en formato decimal. Constan de cuatro valores en los que los dos primeros corresponden al número de red y los dos segundos al de la interfaz de red[5].

Por otra parte los ordenadores también se denomina por referencia a los nombres de dominio. Así, dentro del dominio de la Universitat de València (http://www.uv.es/), una máquina que se denominase pc1 se identificaría por el nombre pc1.uv.es[6]. Estos nombres también son exclusivos, no pueden existir dos máquinas con idéntico nombre.[7]

2 ■ INFORMES JURÍDICOS SOBRE EL NÚMERO IP

El tratamiento de la información generada con motivo del tráfico en internet ha sido objeto de distintos análisis. En este epígrafe se sintetizan algunos de ellos con el objetivo de ofrecer al lector una aproximación a los problemas que se derivan del tratamiento de información relacionado con esta cuestión. Así, se examinarán sucintamente la Consulta 1/1999, el Informe 327/2003 de la Agencia Española de Protección de Datos y distintos documentos del Grupo de Trabajo del art. 29 de la Directiva 95/46/CE[8].

2.1 A LA CONSULTA 1/1999 DE LA FISCALÍA GENERAL DEL ESTADO

Esta conocida consulta no se ocupa específicamente de cuestiones relacionadas con el número IP aunque, como se apreciará, el fondo del asunto consultado si permite establecer un cierto paralelismo entre éste y el número telefónico.

La consulta surgió con motivo de una investigación relacionada con un delito informático. Se requería la identificación de los abonados desde cuyos teléfonos o terminales se habían realizado las conexiones telemáticas. Para ello, el Ministerio Fiscal requirió a la empresa de telecomunicaciones considerando que se trataba de datos de facturación sujetos al régimen de la fenecida LORTAD[9]. Esta Ley, al igual que ocurre con la vigente, establece una comunicación de datos obligatoria a favor de la fiscalía. La compañía operadora consideró que la información solicitada afectaba al secreto de las comunicaciones denegando el acceso a los datos hasta la oportuna resolución judicial.

La Fiscalía General del Estado, FGE en adelante, considera la cuestión a la luz de la doctrina del Tribunal Constitucional y del Tribunal Europeo de Derechos Humanos. Este último en las sentencias Malone y Valenzuela Contreras[10] consideró la existencia de una injerencia de la autoridad pública en la vida privada «el registro mediante aparato contador de los números de teléfono marcados desde un determinado aparato, aun cuando este tipo de vigilancia no implique acceso al contenido de la conversación». En el mismo la STC 114/1984 consideró que la vulneración del secreto de las comunicaciones se produce «por el simple conocimiento antijurídico de lo comunicado –apertura de la correspondencia ajena guardada por el destinatario, por ejemplo–, porque la Constitución protege no sólo el proceso de comunicación, sino también el mensaje, en el caso de que éste se materialice en algún objeto físico, y el objeto del secreto abarca no sólo el contenido de la comunicación sino también otros aspectos de la misma como por ejemplo la identidad subjetiva de los interlocutores o corresponsales».

Ambos argumentos llevan a la FGE a considerar que «no se pueden disociar sin merma relevante de

garantías realidades tan sustancialmente integradas como son el mensaje y su proceso de transmisión».

Ahora bien, la habilitación contenida en la LORTAD, ¿legitimaba al Ministerio Fiscal para recabar de las compañías operadoras datos de tráfico contenidas en los ficheros de facturación? Para responder a esta pregunta la FGE acude al art. 18 CE interpretado a la luz del Convenio núm. 108 del Consejo de Europa[11]. La FGE considera datos sensibles a los datos de tráfico «y en consecuencia sujetos a un régimen muy restrictivo de tratamiento automatizado y de cesión inconsentida». Para llegar a esta conclusión se argumenta que:

«El artículo 11.2 d) LORTAD en cuanto autoriza un flujo inconsentido de información hacia Autoridades no judiciales debe ser interpretado con extraordinaria cautela cuando el dato cuya cesión se pide está protegido «ab origine» por una garantía constitucional autónoma –libertad de conciencia y su correlativo secreto– –art. 16.2 CE–, núcleo duro de la «privacy» –art. 18.1 CE– y, por supuesto, libertad y secreto de las comunicaciones –art. 18.3 CE–, porque si bien el sacrificio del derecho fundamental configurado a partir del artículo 18.4 Constitución Española como derecho a controlar el flujo de las informaciones que conciernan a cada persona –STC 11/1998, de 13 de enero, F. 5– puede ser justo y adecuado cuando dicha información no sea particularmente sensible, el sacrificio de otros derechos fundamentales concurrentes exigirá una previsión legal más específica y concreta –STC 207/1996, F. 6 A– que la que dispensa la cláusula abierta enunciada en el art. 11.2 d) LORTAD.

En relación con los aspectos íntimos de la vida de una persona toda forma de injerencia externa no consentida demanda previsión legal específica y control judicial –STC 207/1996, de 16 de diciembre, F. 4 B–; STC 37/1989, F. 7; STC 7/1994, F. 3; STC 35/1996, F. 2–, de modo que el principio de protección reforzada de los datos sensibles, en el contexto de la doctrina constitucional española, desautoriza todo intento de aplicación indiscriminada a los datos íntimos de las formas legales de cesión previstas con carácter general en el artículo 11.2 LORTAD cuando éstas no sean compatibles con las específicas garantías constitucionales y legales previamente configuradas para preservar la reserva de esos contenidos»

Por otra parte se invoca el art. 11 del Convenio 108 que admite la existencia de formas de protección más amplias y rigurosas que, en nuestro sistema, serían las contempladas por el 18.3 CE[12]. Como corolario y conclusión de la Consulta 1/1999, la Fiscalía General del Estado señala:

"El Ministerio Fiscal no puede inmiscuirse en datos incorporados al contenido sustancial del derecho fundamental al secreto de las comunicaciones sin licencia judicial."

Exigir del operador telefónico la identificación de los números de abonado conectados en una concreta y determinada comunicación supone una restricción de derechos prohibida por el artículo 5.2 EOMF, por lo que es preciso acudir al Juez de Instrucción, justificar la necesidad de la medida e instar la incoación de diligencias previas.

Si el proceso está en curso, el Fiscal también debe solicitar del Juez de instrucción la adopción de la resolución judicial legitimadora de la injerencia.

Ni las diligencias de investigación preprocesal amparadas en los artículos 5 EOMF y 785.bis LECrim, ni las posibilidades de investigación autónoma paraprocesal que cabe deducir de los artículos 781.2 y 792.1.2 LECrim constituyen marco legal idóneo para exigir del operador de la red o del prestador del servicio la revelación de los datos de tráfico registrados en las comunicaciones establecidas».

A la vista de las conclusiones de la FGE sólo cabe hacerse una pregunta. Si en el marco del funcionamiento del protocolo TCP/IP existe un cierto

paralelismo funcional entre un número telefónico y un número IP, ¿qué régimen jurídico se le aplicará?

2.2 EL INFORME 327/2003 DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS.[13]

En este informe la AEPD responde a una consulta en la que se le interrogaba sobre distintas cuestiones relativas a la consideración como dato de carácter personal de una dirección IP[14]. Se trataba, entre otros aspectos de determinar la aplicabilidad de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)y del Reglamento de Medidas de Seguridad[15]. La Agencia parte de la definición de dato personal del art 3 a), esto es será un dato «cualquier información concerniente a personas físicas identificadas o identificables». A continuación se examina el funcionamiento del Protocolo TCP/IP en términos muy similares a los utilizados en el primer epígrafe de este trabajo. La AEPD considera, habida cuenta del funcionamiento técnico descrito, que los proveedores de acceso a Internet (ISP) y los administradores de redes locales pueden identificar por medios razonables a los usuarios de Internet a los que han asignado direcciones IP. Es más los ISP suelen disponer de un fichero histórico con el registro de las sesiones de los usuarios[16] y, en caso de que se utilice una red pública de telecomunicaciones, mediante telefonía convencional o móvil, la operadora registra el número marcado, junto con la fecha, la hora y la duración, para la posterior facturación.

En consecuencia, si se acude al ISP para contrastar un determinado número IP aquél estará en condiciones de identificar a un usuario de Internet por medios razonables. Por tanto, según la AEPD «se puede hablar de datos de carácter personal en el sentido de la letra a) del artículo 3 de la Ley 15/1999».

Para los terceros la identificación de un sujeto a partir de la IP resulta más compleja. Si bien se puede identificar el número no resulta tan sencillo relacionarlo con la identidad del usuario, especialmente cuando la IP se asigna de forma dinámica caducando con cada sesión. No obstante subraya la Agencia:

«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».

La conclusión que de estas premisas se derivan resulta bastante evidente: «las direcciones IP tanto fijas como dinámicas, con independencia del tipo de acceso, se consideran datos de carácter personal resultando de aplicación la normativa sobre protección de datos»[17]. Asimismo, la AEPD también considera datos personales a los necesarios para la autentificación del usuario indicando que:

«En cuanto a la consideración de los "log-in[18]" de acceso a Internet o a páginas personales como datos de carácter personal, resultarán de aplicación las consideraciones que se realizan en párrafos anteriores. Si identifica de forma directa al usuario, no hay duda de que estaremos ante un dato de carácter personal, por el contrario si este es anónimo, en principio no sería un dato de carácter personal, pero si, por ejemplo, el proveedor de servicios de Internet a través de ese "log in", puede identificar al usuario con el que tiene un contrato de acceso a Internet, sí será considerado como un dato de carácter personal».

En sus Recomendaciones al sector del comercio electrónico[19], la AEPD no reflexiona tanto sobre la IP como sobre determinados tratamientos invisibles[20] como las *cookies*[21]. Las empresas depositan estos

archivos en el ordenador personal del cliente para identificarle en una posterior conexión sin necesidad de articular ningún proceso de autentificación. En el párrafo cuarto de la Tercera Recomendación se plantea la necesidad de informar sobre este tipo de tratamientos:

«Si, aparte de los datos personales que facilita voluntariamente el interesado a través de Internet, se utilizan procedimientos automáticos invisibles de recogida de datos relativos a una persona identificada o identificable (cookies, datos de navegación, información proporcionada por los navegadores, contenidos activos,...) se informará claramente de esta circunstancia al usuario, antes de comenzar la recogida de datos a través de ellos o de desencadenar la conexión del ordenador del usuario con otro sitio web.

Así mismo, se deberá informar al afectado del nombre de dominio del servidor que transmite o activa los procedimientos automáticos de recogida, de la finalidad de los mismos, de su plazo de validez, de si es necesaria o no la aceptación de dichos procedimientos para visitar el sito web y de la opción de que dispone todo usuario de oponerse a esta modalidad de tratamiento, además de las consecuencias de desactivar la ejecución de dichos procedimientos, cuando dicha opción esté disponible para el usuario».

En consecuencia, y puesto que el número IP se transmite automáticamente con la conexión del ordenador[22] cliente al servidor y además se suele asociar al conjunto de la navegación tanto para facilitarla como para establecer un perfil de usuario, la Agencia considera necesario informar al respecto en el momento de la recogida de tales datos. Asimismo, procederá aplicar a tales datos las previsiones de la LOPD en un contexto, como el de internet, en el que la información circula por múltiples Estados.

En este sentido la Agencia en la segunda versión de sus Recomendaciones a usuarios de Internet alerta sobre las posibilidades que ofrece el seguimiento subrepticio de la navegación de los usuarios mediante cookies o la explotación del clickstream mediante herramientas convencionales o de webmining así como los programas espía o spyware[23].

En los distintos documentos que hemos examinado la Agencia Española de Protección de Datos responde a una única cuestión: ¿es la IP un dato personal? No podía ser de otro modo habida cuenta de su naturaleza y funciones. Sin embargo, la respuesta no puede, o al menos no debería ser tan lineal ya que nos encontramos, probablemente, ante una superposición de normas aplicables. ¿Qué ocurre si la IP además de un dato de carácter personal constituye un elemento del funcionamiento de un protocolo de comunicaciones en internet? ¿Serían aplicables las previsiones jurisprudenciales que rigen la práctica de las interceptaciones basadas en la técnica del comptage? Y, en tal caso, ¿operaría algún principio de determinación de la norma aplicable?

2.3 LOS DOCUMENTOS DEL GRUPO DE TRABAJO SOBRE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES (GDT)

El GdT se ha preocupado en distintos documentos de todo lo que concierne al tratamiento de datos de carácter personal en internet[24]. En este sentido se ha ocupado de estudiar el propio funcionamiento de las comunicaciones en la red, de identificar condiciones de privacidad jurídica y tecnológica[25], y del uso y tratamientos de datos en contextos específicos como el comercio electrónico[26], el tráfico en las comunicaciones[27] y en la vigilancia empresarial[28].

Seguramente el documento más completo, y complejo, sobre esta materia sea el Documento de Trabajo sobre Privacidad en Internet[29]. En el se analizan todos y cada uno de los servicios que nos ofrecen las tecnologías de la información y las comu-

nicaciones con un diagnóstico de los riesgos que comportan al que se acompañan recomendaciones básicas. Así ocurre respecto del Protocolo TCP/IP señalándose, entre otros riesgos los vinculados al funcionamiento del Protocolo, como la circulación de información por países no seguros, la localización de usuarios conectados o el seguimiento de la navegación mediante el almacenamiento de los nombres de dominio de los websites visitados. Hay que tener en cuenta, que en el marco de la navegación en internet la IP asignada opera como el primer criterio de identificación. En este sentido el rango de la IP permitirá al proveedor, al titular de un portal y al anunciante obtener información acerca del proveedor del acceso[30]. Éste es un dato que puede ser muy valioso para elaborar perfiles ya que si, por ejemplo, un profesor de universidad navega desde el entorno de la institución en la que trabaja su IP identifica a ésta. Además los servidores vinculados a la navegación, y también software específico como Alexa o Google, pueden almacenar información sobre los lugares visitados.

Tanto en este documento como en recomendaciones y dictámenes anteriores, y posteriores, puede subrayarse que las conclusiones del Grupo apuntan siempre en una misma dirección. Se identifica con claridad aquellos casos en los que resultan de aplicación las Directivas vigentes en la materia[31], se recomienda garantizar el anonimato de los usuarios[32] y se establecen recomendaciones y pautas de actuación al respecto.

En este sentido, el Grupo ha establecido indicaciones sobre la recogida de datos en línea[33] señalando en lo que aquí interesa la aplicabilidad de los principios vigentes en materia de protección de datos –consentimiento, información en la recogida, derechos de los titulares etc.– y estableciendo indicaciones específicas para el caso así como la necesidad de

«12. Mencionar con claridad la existencia de procedimientos automáticos de recogida de datos, antes de usar dichos métodos.

(…).La información y la posibilidad de oponerse a la recogida deberán comunicarse antes de utilizar cualquier procedimiento automático que desencadene la conexión del ordenador del usuario con otro sitio Web, por ejemplo, cuando un sitio Web conecta automáticamente al usuario a otro sitio para mostrarle publicidad en forma de *pancarta* publicitaria, con el fin de evitar que este segundo sitio recopile datos sin que el usuario sea consciente de ello.»[34].

La información deberá ofrecerse en los siguientes términos:

«17. en la página inicial del sitio y en todos los lugares donde se recojan datos personales en línea deberá poderse acceder directamente a información completa sobre la política de protección de la intimidad (incluida la forma de ejercer el derecho de acceso). El título del encabezado que deba seleccionarse con el ratón deberá estar resaltado, ser explícito y específico, de manera que transmita al usuario de Internet una idea clara del contenido que se le va a mostrar. Por ejemplo, el encabezado podría indicar «Esta página recoge y trata datos personales relacionados con usted. Si desea más información, pinche aquí» o bien «Protección de datos personales o de la intimidad». También deberá ser lo bastante específico el contenido de la información a la que se dirige el usuario de Internet».

En lo que al número IP concierne el GdT se ha preocupado de la evolución del Protocolo TCP/IP (Ipv6) afirmando de modo categórico el carácter de dato personal que posee el identificador IP y destacando los riesgos derivados de la aparición de identificadores estáticos.

El documento suscribe las conclusiones de la "31ª Reunión del Grupo de Trabajo Internacional de Protección de Datos en las Telecomunicaciones", celebrada los días 26 y 27 de marzo de 2002 en Auckland. Este Grupo identificó distintos riesgos ligados al futuro funcionamiento del Protocolo. Entre ellos cabe destacar la mayor facilidad para elaborar

perfiles basándose en número IP estático y la dirección de la tarjeta ethernet del ordenador del usuario que permite la comunicación y las consecuencias que esto tiene al trasladarse el protocolo a otro tipo de comunicaciones. De tales conclusiones conviene destacar las relativas los principios sobre protección de datos aplicables al Ipv6:

«La infraestructura y los aparatos técnicos de telecomunicaciones deben diseñarse de tal forma que no se utilice ningún dato personal o se emplee el menor número técnicamente posible de datos personales para el funcionamiento de redes y servicios. El identificador único de una interfaz, tal como se integra en el IPv6, constituiría un identificador de aplicación general.

En contradicción con el principio de minimalización de los datos, este uso de un identificador único constituye un riesgo de elaboración de perfiles de las personas basado en el conjunto de sus actividades relacionadas con una red.

La protección del derecho fundamental a la privacidad frente a este riesgo de elaboración de perfiles debe primar a la hora de analizar los distintos aspectos del nuevo protocolo como, por ejemplo, su sistema de gestión.

Los datos de tráfico y, en particular, los datos sobre la localización, merecen una protección específica dado su carácter sensible.

Si la información sobre la localización tiene que generarse en el marco de la utilización de aparatos móviles y de otros objetos conectados mediante el IP, esta información deberá protegerse contra la intercepción ilegal y la utilización abusiva.

También debe evitarse que la información sobre la localización (y el cambio de esta información sobre la localización en función del movimiento del usuario del móvil) se trasmita sin codificar al destinatario de la información a través del encabezamiento de la dirección IP utilizada.

Los protocolos, productos y servicios deberán diseñarse de forma que se puedan elegir direcciones permanentes o provisionales. Los parámetros predefinidos deberían permitir un nivel elevado de protección de la privacidad».

En resumen, en el texto de la reunión de Auckland reproducido en la Recomendación, se identifican riesgos para el derecho fundamental a la protección de datos, el secreto de las comunicaciones y la vida privada así como para la libertad de circulación en la medida en la que los nuevos dispositivos móviles permiten localizar a sus portadores[35].

Ahora bien, el tratamiento de los datos de tráfico en las comunicaciones posee una relevancia adicional cuando se trata del empleo de tales datos en el contexto de una interceptación de las telecomunicaciones. Respecto de esta hipótesis el Grupo ha subrayado la necesidad de respetar los requisitos que el Tribunal Europeo de Derechos Humanos ha venido señalando en su jurisprudencia sobre límites al derecho a la vida privada con fundamento en el artículo 8.2 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, esto es la invocación de un fundamento jurídico, la necesidad de la medida limitadora en una sociedad democrática y la conformidad con alguno de los objetivos legítimos enumerados en el Convenio[36].

Por su parte, los operadores de telecomunicaciones y los proveedores de servicios deberían cancelar y/o tornar anónimos los datos relativos al tráfico y la facturación en cuanto termine la comunicación de modo que «las finalidades para las cuales pueden tratarse los datos, la duración de su posible conservación, así como el acceso a dichos datos estén estrictamente limitados» y adoptar las medidas necesarias con el fin de hacer técnicamente difíciles o imposibles, según el estado actual de la técnica, la interceptación de las telecomunicaciones por instancias no autorizadas por la ley. Cuando por el contrario deba facilitarse tal interceptación «no debe tener por consecuencia reducir el nivel general de

confidencialidad de las comunicaciones y de protección de la intimidad de las personas», señalándose la necesidad de prestar una atención particular a la utilización de satélites o de Internet[37]. Por último, y con carácter general se señala la necesidad de prohibir la vigilancia exploratoria o general de las telecomunicaciones a gran escala[38].

El GdT se ha ocupado también del supuesto específico de la conservación de los datos de tráfico en cumplimiento de las legislaciones nacionales[39] afirmando la aplicabilidad a esta materia tanto de la Directiva 97/66/CE, –hoy ya la D/2002/58/CE–, específica de este sector, como la Directiva 95/46/CE, y, reiterando su planteamiento sobre los límites al derecho a la vida privada. El Grupo ha recomendado la no conservación de los datos de tráfico de las telecomunicaciones a efectos exclusivos de control y la conservación por el tiempo estrictamente necesario para las necesidades derivadas de la facturación y la protección de los derechos del consumidor[40].

Del conjunto de documentos puede concluirse que el Grupo de Trabajo ha buscado el modo de articular mecanismos jurídicos de protección de la vida privada en internet en todas sus dimensiones. En lo que respecta al número IP el GdT ha distinguido en términos objetivos aquellos supuestos en los que se practica una interceptación de las comunicaciones de aquellos otros en los que se indexa y trata dicho número en una base de datos. En el último caso se distinguen netamente dos supuestos. El primero es el tratamiento del número IP por las operadoras o proveedores con fines de tráfico y facturación. El segundo se refiere a los tratamientos que vinculan la IP a navegaciones concretas para elaborar perfiles de usuario, generalmente con fines comerciales y publicitarios. Respecto del primero de los supuestos definidos, el Grupo ha postulado la aplicación de la doctrina del TEDH sobre el secreto de las comunicaciones y la Directiva sobre privacidad en las telecomunicaciones[41]. En el segundo caso se apuesta claramente por la aplicación de las normas que regulan la protección de datos personales.

3 ■ CONSECUENCIAS JURÍDICAS: EL DERECHO APLICABLE

El número IP, tecnológicamente hablando, puede parecer una cuestión menor carente de no más relevancia jurídica que la que deriva de su conceptuación como dato de carácter personal. Es más, no es infrecuente que en los foros tecnológicos se tenga en poca consideración la preocupación de los juristas por esta cifra. Sin embargo, el contexto social que nace con internet plantea problemas nada desdeñables respecto de los que el número IP no es ni más ni menos que el punto de partida para aplicar tecnologías orientadas al control social, al análisis de los patrones de conducta de los sujetos en la red de redes. Sin ánimo de agotar las posibilidades existentes[42], baste con citar tres ámbitos en los que estos controles pueden comprometer derechos fundamentales. Así, en primer lugar, cabe referirse al ámbito laboral en donde las facultades de control del empresario plantean situaciones de conflicto y la necesidad de garantizar la eficacia horizontal de los derechos a la intimidad y al secreto de las comunicaciones y balancearlos con los derechos patronales[43]. Por otra parte, ya se ha subrayado el valor comercial que adquiere el análisis de la navegación[44] al que sin ningún género de dudas se unirán en breve las posibilidades que ofrece la domótica[45]. Por último, cabe referirse a la tendencia legislativa y política hacía el control de las redes que se consolida y justifica tras los atentados del 11 de septiembre de 2001[46]. Precisamente este último elemento, dota de la máxima relevancia jurídica a la cuestión ya que todo seguimiento de un sujeto en internet, –ya sea de su navegación, de su correo electrónico o de sus transferencias de ficheros etc.–, parte de la identificación de la IP de su ordenador.

Por tanto, y a la vista de las posibilidades que se apuntan, cabe considerar el número IP desde la doble perspectiva del bien jurídico protegido, la vida privada, y del Derecho aplicable que será, según los casos, el régimen jurídico previsto para el secreto de

las comunicaciones o el concerniente al derecho fundamental a la protección de datos.

3.1 VIDA PRIVADA EN LA SOCIEDAD DE LA INFORMACIÓN

En Internet la información personal constituye la fuente de riqueza por excelencia en lo que Castells denomina muy gráficamente como "Galaxia Internet"[47]. Así, si se diseccionan los componentes últimos de la sociedad de la información hasta reducirlos a sus elementos esenciales se llega básicamente a dos: información personal y conocimiento.

El tratamiento de la información personal encuentra acomodo en el artículo 18 de la Constitución Española que abarca las múltiples manifestaciones posibles de la vida privada y de la personalidad, –la intimidad personal y familiar, el honor, la imagen, la inviolabilidad del domicilio y el secreto de las comunicaciones–, y las dota de relevancia constitucional. El artículo 18 CE cumple así un papel instrumental esencial en la protección jurídica de los derechos fundamentales en su relación con las tecnologías de la información y las comunicaciones. Todos los derechos del artículo 18 de la Constitución Española giran en torno a la vida privada[48] de modo que ésta se configura implícitamente como un bien constitucionalmente protegido y autónomo respecto de ellos. De esta manera, todos aquellos supuestos pertenecientes a la vida privada que no encontrasen cobertura en cualquiera de las previsiones del artículo 18 C.E. deberían incluirse en la noción legal y constitucional de la vida privada y ello define a la par un sustrato común para los derechos del citado precepto.[49]

3.2 NÚMERO IP Y PROTECCIÓN DE DATOS

A la luz de los textos e informes arriba expuestos y, por supuesto de las normas jurídicas que interpretan parece evidente que el número IP constituye un dato de carácter personal. Por tanto, el tratamiento de tal dato comportará la aplicación al mismo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y de sus homónimas europeas que transponen la Directiva 95/46/CE.

Ahora bien, esta afirmación debe matizarse ya que una interpretación literal de esta afirmación tendría, posiblemente, consecuencias no del todo deseables. En principio, la existencia de legislación sobre protección de datos y el reconocimiento por la jurisprudencia del Tribunal Constitucional de un derecho fundamental a su protección[50] suponen que todo tratamiento de datos personales, sea o no en Internet, dependa del consentimiento libre e informado del afectado. La libertad y la dignidad individual exigen que el sujeto tenga la posibilidad de autodeterminarse conscientemente[51], de elegir en libertad y de ejercer un control real sobre su información personal. Ahora bien, ¿qué ocurre cuando el sujeto no es consciente de prácticas cuyo objeto no es otro que rastrear su "navegación". Por otra parte, y en este contexto, resulta necesario abordar una cuestión extrajurídica que sin embargo comporta un cierto grado de normación de la conducta del individuo. Como Lessig ha venido a afirmar de un modo particularmente gráfico, en Internet la ley es el código informático. Dicho de otra forma, el modo en que un individuo se conecta, el tipo de uso que el sistema le permite o los hábitos y comportamientos de las comunidades virtuales, en una gran parte de los casos vienen predefinidos por las posibilidades y limitaciones que impone la programación informática. En consecuencia, procederá estudiar el grado de autodeterminación posible en este contexto.

Por otra parte, cabría plantearse hasta que punto en Internet el individuo se encuentra protegido frente a las condiciones generales de contratación que imponen las empresas y frente a las prácticas existentes en Internet. Por una parte, deben enunciarse a título de ejemplo las prácticas del "o lo

tomas o lo dejas" ("*take it or leave it*") que restringen cualquier posibilidad de elección. Por otra parte, en el modelo actual la actuación de proveedores, portales y sites, implica una seria dificultad para el internauta de mantener un razonable nivel de anonimato[52].

En este sentido, y como primera conclusión resulta bastante evidente que si bien las normas sobre protección de datos ofrecen una cierta tutela esta podría ser ineficiente en aquellos ámbitos en los que la situación del sujeto es de debilidad. Así en el ámbito laboral, y en general, en el de las relaciones jurídicas vinculadas a las transacciones comerciales el sujeto renunciará con mucha facilidad a su propia autodeterminación. Esta renuncia, las más de las veces se basa en la imposibilidad de "negociar" con quienes establecen controles sobre los usos del ordenador vinculados al número IP ya sea por razones de control empresarial, ya sea por razones publicitarias[53].

3.3 EL SECRETO DE LAS COMUNICACIONES

Tanto el Tribunal Constitucional, como la doctrina[54], han definido tempranamente las notas características del secreto de las comunicaciones. En el fundamento jurídico séptimo de la STC 114/1984, *caso Póveda Navarro contra el diario «Información»*,[55] señaló varias de estas características. En primer lugar, el derecho «consagra la libertad de las comunicaciones, implícitamente, y, de modo expreso, su secreto», de modo que se vulnera con «la interdicción de la interceptación o del conocimiento antijurídicos de las comunicaciones ajenas». Así «el derecho puede conculcarse tanto por la interceptación en sentido estricto (que suponga aprehensión física del soporte del mensaje –con conocimiento o no del mismo– o captación, de otra forma, del proceso de comunicación) como por el simple conocimiento antijurídico de lo comunicado (apertura de la correspondencia ajena guardada por su destinatario, por ejemplo)» [56].

Además, «el concepto de «secreto», que aparece en el artículo 18.3 CE, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como, por ejemplo, la identidad subjetiva de los interlocutores o de los corresponsales» e incluso, se refiere el Tribunal Constitucional al comptage que «permite registrar cuáles hayan sido los número telefónicos marcados sobre un determinado aparato, aunque no el contenido de la comunicación misma». Así pues de lo que se trata es de garantizar la comunicación, asegurar «su impenetrabilidad por terceros ajenos a la comunicación misma».

El secreto del art. 18.3 tiene un carácter «formal», «en el sentido de que se predica de lo comunicado, sea cual sea su contenido y pertenezca o no el objeto de la comunicación misma al ámbito de lo personal, lo íntimo o lo reservado», opera mediante «la presunción iuris et de iure de que lo comunicado es «secreto», en un sentido sustancial». No obstante, el secreto de las comunicaciones no se proyecta sobre los interlocutores sobre los cuales puede pesar la obligación de no revelar lo comunicado so pena de vulnerar el derecho a la intimidad de alguno de ellos.

En cualquier caso, y como señala el fundamento jurídico cuarto de la STC 34/1996, el secreto de las comunicaciones constituye una de las «manifestaciones fenoménicas» del derecho a la intimidad.

Por último el Tribunal Constitucional, cuando se trata de tutelar el secreto de las comunicaciones no se prejuzga el concreto medio tecnológico empleado. Es más, en el fundamento jurídico sexto de la STC 81/1998, se alerta frente a los nuevos riesgos para el secreto de las comunicaciones asociados al progreso tecnológico y subraya el papel instrumental que el derecho a la intimidad juega respecto del entero sistema de derechos fundamentales:

«El análisis ha de partir aquí del hecho de que la necesidad de tutela del derecho fundamental al secreto de las comunicaciones telefónicas es

especialmente intensa, tanto porque dicho derecho, a consecuencia de los avances tecnológicos, resulta fácilmente vulnerable, cuanto porque constituye una barrera de protección de la intimidad, sin cuya vigencia efectiva podría vaciarse de contenido el sistema entero de los derechos fundamentales. (...) »

Finalmente el Alto Tribunal en las SSTC 70/2002 y 123/2002 ealiza una interpretación del derecho tecnológicamente actualizado entendiendo que tutela frente a las interferencias en todo tipo de comunicación «cualquiera que sea la técnica de transmisión utilizada» y con independencia del contenido del mensaje: «conversaciones, informaciones, datos, imágenes, votos, etc.». El fundamento jurídico sexto de la segunda de las sentencias citadas establece sin embargo una cierta gradación en la intensidad de la tutela distinguiendo entre la comunicación en si misma y los datos de tráfico que genera lo que le permite posteriormente modular y aceptar una entrega de datos de facturación a la policía autorizada mediante providencia[57].

Así, de la configuración constitucional del secreto de las comunicaciones se deduce su versatilidad para ofrecer una suerte de defensa adelantada que sólo dependerá de un dato objetivo: la existencia de comunicación. Este planteamiento no excluye, en absoluto la aplicación de la legislación vigente en materia de protección de datos pero si establece una suerte de precedencia aplicativa respecto de estas normas[58].

4 ■ BREVE CONCLUSIÓN

Difícilmente, puede alcanzarse una conclusión concluyente en esta materia en la que, sin lugar a dudas, existen multitud de elementos discutibles. De una parte, más allá de establecer si el número IP forma parte del bien jurídico protegido por el secreto de las comunicaciones, deberá identificarse que tipo de comunicación en internet merece ser considerada como tal. En este sentido, de los múltiples servicios asociados a internet parece evidente que el correo electrónico, la telefonía IP y los canales privados de conversación, –salas privadas de chat, los programas de mensajería o el envío de sms,– se encontrarán obviamente potegidos por este derecho. Sin embargo, ¿existe comunicación en la simple navegación y en la descarga o intercambio de ficheros[59]?

Los informes del Grupo de Trabajo detectan riesgos ciertos para la vida privada de los ciudadanos en internet y apuntan claramente en la dirección de articular una doble barrera de protección en la que la garantía del secreto de las comunicaciones juegue un papel determinante inicial y en la que se apliquen en todo caso las normas sobre protección de datos a los ficheros en los que se almacena tal información ■

Notas

1 Acrónimo que deriva de la expresión "*Local Area Network*"

2 Acrónimo que deriva de la expresión "*Wide Area Network*".

3 Lawrence Lessig ha descrito muy gráficamente hasta que punto la programación informática de los espacios web, de las intranet y en general de las comunidades virtuales posee aspectos muy cercanos a la estructura y funcionamiento de las normas jurídicas. LESSIG, LAWRENCE. *El código y otras leyes del ciberespacio*. Taurus, Madrid, 2001

4 Acrónimo que deriva de la expresión *"Transmission Control Protocol"*.

5 Obviamente se necesita alguna cosa más. La información es dirigida mediante routers, o encaminadores, a través de los que aquella pasa hasta alcanzar su destino. Además la información no viaja de una sola vez sino que se divide en paquetes mediante la denominada conmutación de paquetes. Cada paquete contiene sólo una parte del total de información que se transmite junto con los datos que la identifican, los necesarios para la propia transmisión y las direcciones IP del remitente y el destinatario.El proceso de encaminamiento depende del protocolo IP: El protocolo TCP es el que permite que los ordenadores se comuniquen entre sí. Él es el que divide, codifica la información en el emisor y la descodifica en el receptor.

6 Para traducir los nombres por dominio a sus correspondientes números IP existen los servidores de nombres de dominio (DNS servers).

7 Véase el tutorial sobre el protocolo TCP/IP disponible en el website del Departamento de Ingeniería y Tecnología de Computadores de la Universidad de Murcia, (disponible el 01/01/2004). http://ditec.um.es/laso/docs/tut-tcpip/3376c22.html#figipaddrc y el interesante manual CTI. *Introducción a las redes de ordenadores. Introducción a Internet*. Centro de Tecnología Informática de la Universidad de Navarra. http://www.unav.es/cti/manuales/pdf/redesinternet.pdf

Por último, debe citarse documento de trabajo sobre Privacidad en internet elaborado por el GDT ya que liga las cuestiones técnicas con consideraciones jurídicas de muy alto nivel. GdT. Documento de Trabajo, de 21 de noviembre de 2000, Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. 5063/00/ES/Final (WP 37).

8 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de julio de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (D.O.C.E. serie L. núm. 281, de 23 de noviembre de 1995).

9 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de dos Datos de Carácter Personal. (B.O.E. núm. 262, de 31 de octubre).

SSTEDH Malone c. Royaume-Uni, Serie A núm. 82 (1984) y Valenzuela Contreras c. Espagne, Recueil 1998-V (1998).

10 Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, ratificado por Instrumento de 27 de enero de 1984.

11 La FGE aporta aquí una interesante reflexión:

«Como explica la exposición de motivos de la LORTAD, el desarrollo legislativo del artículo 18.4 Constitución Española ha implicado la atribución de un nuevo derecho al ciudadano cuyo objeto de protección es la privacidad, ya que la intimidad en sentido estricto está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 Constitución Española y por las leyes que los desarrollan.

Se ha creado por ello un ámbito nuevo de inmunidad en la medida en que las garantías constitucionales clásicas se han revelado insuficientes para defender al ciudadano de la insidiosa influencia que la nueva técnica puede ejercer en detrimento del concepto más amplio de privacidad, pero no se liquida por ello la vigencia de los instrumentos específicos de protección de la intimidad, entre los cuales ocupa un puesto preeminente la necesidad de licencia judicial para alzar el secreto que ampara las comunicaciones telefónicas».

12 Disponible en https://www.agpd.es/index.php?idSeccion=390. Asimismo puede consultarse una referencia a esta cuestión en AEPD. *Memoria de 2003*. Pág. 81.

13 La preocupación de la AEPD por estas cuestiones es muy anterior. Existen así unas Recomendaciones a usuarios de internet de 1999. Por otra parte, según la Memoria del año 2000, la Subdirección General de Inspección de Datos analizó 44 webs pertenecientes a empresas dedicadas al comercio electrónico que, en lo que afecta a este trabajo constató prácticas de redireccionamiento del usuario de modo que «en ocasiones, el usuario crea estar facilitando sus datos personales a una entidad cuando en realidad es otra (radicada probablemente en otro lugar del mundo) la que los está obteniendo, siendo muchos los casos en los que ésta última no se identifica claramente en la Web».

AEPD. *Memoria 2000* p. 185.

Asimismo, en la Memoria correspondiente al año 2001, en la sección dedicada a la Subdirección del Registro General de Protección de Datos, y en concreto en el epígrafe 4.2 dedicada a la declaración de tratamientos en Internet llama poderosamente la atención la ausencia de declarantes que incluyan en el formulario de inscripción referencias a tratamientos invisibles. La Agencia apuesta por una clara política de transparencia recomendando ofrecer:

«7. Información referente al uso de tratamientos invisibles, bien sea para, informar de que no utiliza este tipo de tratamientos o, en el caso de que los utilizara, una indicación de la finalidad de los mismos y una solicitud del consentimiento. Algunos responsables incluyen información acerca de las opciones que incluyen los navegadores con relación a las "cookies", para que los usuarios puedan aceptar o no el envío de las mismas»

AEPD. *Memoria 2001*, p. 94 y ss.

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

15 En concreto se afirma que «Un proveedor de acceso a Internet que tiene un contrato con un abonado a Internet, normalmente mantiene un fichero histórico con la dirección IP (fija o dinámica) asignada, el número de identificación del suscriptor, la fecha la hora y la duración de la asignación de dirección».

16 Particular interés reviste esta utilidad para las empresas dedicadas a gestionar “banners”, esto es anuncios digitales personalizados. Resulta interesante la descripción sobre el funcionamiento del sistema de DoubleClick que ofrecen Gauthronet y Nathan:

«Le mécanisme d’affichage des bannières publicitaires suppose une série de relations tripartites entre le site Web visité par l’utilisateur, son browser et les serveurs de DoubleClick à New York ou de GlobalTrack à Austin. Aussitôt qu’un utilisateur est connecté, le site d’accueil affiche une page dans laquelle apparaissent des espaces réservés pour l’incrustation de bannières publicitaires. Le browser initie une requête auprès du serveur du prestataire afin de récupérer le fichier graphique qu’il doit incruster dans la page Web en cours de chargement. Pour déterminer quelle est la bannière pertinente à afficher, le serveur du prestataire récupère l’information persistante du browser (adresse IP de l’utilisateur, adresse du réseau, nom de son entreprise...), analyse le contenu de la page Web sur laquelle se trouve l’utilisateur et détermine parmi le millier de bannières qu’il a en stock quelles sont celles susceptibles de lui être envoyées ; plus précisément le serveur du prestataire indique au browser de l’utilisateur quelle requête HTTP il doit lui adresser ; tout ce processus s’opère théoriquement en guère plus de 20 millisecondes.(...)

Les serveurs continuent pendant ce temps là à collecter et à assembler de l’information: ils référencent le contenu du site visité par l’utilisateur, ainsi que plus particulièrement les pages qu’il a chargées, et à l’intérieur de ces pages, ils identifient les mots-clés devant servir plus tard à déterminer encore plus précisément la pertinence du lieu d’affichage des bannières. DoubleClick affecte alors un n° d’identification spécifique et permanent à l’utilisateur ; ce numéro, si son browser le lui permet, lui est transmis à travers un cookie: cela permettra ensuite de déterminer avec certitude combien de fois une bannière a été vue par un utilisateur donné. On peut également faire l’hypothèse que ce n° d’identification va permettre, au fur et à mesure des sessions de l’utilisateur dont DoubleClick aura connaissance, de compléter et d’affiner les données de son profil».

Gauthronet, Serge y Nathan, Frédéric. *Les services en ligne et la protection des données et de la vie privée*. Etude pour la Commission des Communautés Européennes (DG XV). ARETE, Coopérative Informatique, 1998, págs. 32 y 33

17 La siguiente consecuencia lógica no es otra que la aplicación de medidas de seguridad:

«En este sentido un fichero que contuviera únicamente las direcciones IP, en principio resultaría de aplicación las medidas de seguridad nivel básico. Por el contrario un fichero que contuviera la dirección IP asociada, por ejemplo, a los sitios web solicitados con la finalidad de elaborar un determinado perfil del usuario, si el mismo permite obtener una evaluación de la personalidad del individuo, se deberán adoptar las medidas de seguridad nivel medio. Con ello queremos decir que, deberán implementarse sobre fichero los dispositivos técnicos que garanticen los niveles de seguridad que especifica el 4 del Reglamento, atendiendo a la naturaleza de la información tratada, y en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información».

18 N. del A. La expresión log-in significa literalmente entrar en el sistema".

19 Recomendaciones de la Agencia de Protección de Datos al sector del comercio electrónico, para la adecuación de su funcionamiento a la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (año 2000). Disponibles en https://www.agpd.es/upload/recomendaciones_comercio_electronico_pdf.pdf.

20 Véase mi trabajo Martínez Martínez, Ricard.«Vida privada en Internet» en *Revista datos personales.org, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 7, enero de 2004. Disponible en el website de la Revista http://www.madrid.org/comun/datospersonales/0,3126,457237_0_127535941_12151300_12145900,00.html

21 En el Código Ético de Comercio Electrónico y Publicidad Interactiva las cookies se definen como « pequeños ficheros de datos generados a través de instrucciones enviadas por los servidores web a los programas navegadores de los usuarios, y que se guardan en un directorio específico del terminal de aquéllos, con el objetivo de reunir información compilada por el propio fichero».
https://www.agpd.es/upload/RGPD/CODIGOS%20TIPO/C%D3DIGO%20Comercio%20Electr%F3nico%20y%20Publicidad%20Interactiva.pdf

22 Una exposición sobre la transmisión de información del cliente al servidor acompañada de un ejemplo muy gráfico con el propio ordenador del visitante se encuentra en el sitio oficial De la Comisión Nacional Informática y Libertades de Francia. (http://www.cnil.fr/index.php?id=19) .

23 En este sentido las recomendaciones que ofrece son de naturaleza estrictamente práctica, verificar el titular del website y sus políticas de privacidad– o técnica, –procurar la utilización de servidores anónimos, criptografía, programas anti-cookies etc.–. Así se señala a título de ejemplo:

«Cuando navegue por Internet, sea consciente de que los servidores Web que visita pueden registrar tanto las páginas a las que accede como la frecuencia y los temas o materias por las que busca, aunque no le informen de ello. En el caso de que no desee dejar constancia de sus actividades, utilice herramientas y servidores que preserven su identidad, generalmente proporcionándole un pseudónimo que, en función de las distintas legislaciones y en determinadas circunstancias, podría ser revelado».

AEPD. Recomendaciones a usuarios de Internet, ed. 2002, pág 4 y ss.. Disponible en
https://www.agpd.es/upload/Recomendaciones_Internet_2001%20_V3.pdf.

24 GdT. Documento de Trabajo, de 23 de febrero de 1999, sobre Tratamiento de datos personales en Internet. Doc. 5013/99/ES/final WP 16.

25 Dictamen 1/1998, de 16 de junio, sobre Plataforma de Preferencias de privacidad (P3) y la Norma de Perfiles Abierta (OPS). Doc XV D/5032/98 WP 11.

26 Dictámen 1/2000 sobre determinados aspectos de la protección de datos del comercio electrónico. Doc. 5007/00/ES/final WP28

27 GdT ya que liga las cuestiones técnicas con consideraciones jurídicas de muy alto nivel. GdT. Documento de Trabajo, de 21 de noviembre de 2000, Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. 5063/00/ES/Final (WP 37).

GdT. Documento de trabajo, de 25 de noviembre de 2002, relativo al tratamiento de datos personales mediante vigilancia por videocámara. Doc. 11750/02/ES (WP 67) y GdT. Documento de trabajo de 29 de mayo de 2002 relativo a la vigilancia de las comunicaciones electrónicas en el lugar de trabajo. Doc. 5401/01/ES/Final (WP 55)

28 GDT. Documento de Trabajo, de 21 de noviembre de 2000, Privacidad en Internet: Enfoque comunitario integrado de la protección de datos en línea. 5063/00/ES/Final (WP 37).

Schwartz ha subrayado el proceso de mercantilización de la vida privada que se esta producuiendo de la mano de Internet. Esto estimula una visión propietaria de la privacy más cercana al derecho de propiedad intelectual en la que los más poderosos imponen sus condiciones a los usuarios.

Así:

«The leading paradigm on the Internet and in the real, or offline world, conceives of privacy as a personal right to control the use of one's data. I refer to this idea as "privacy-control." This liberal autonomy principle seeks to place the individual at the center of decision-making about personal information use. Privacy-control seeks to achieve informational self-determination through individual stewardship of personal data, and by keeping information isolated from access. Privacy-control also encourages a property approach to personal information that transforms data into a commodity. Finally, the privacy-control paradigm supports a move to an intellectual property regime for privacy. This regime would center itself around a view of personal information as a resource to be assigned either to the person to whom it refers, or to a marketing company or other commercial entity».

SCHWARTZ, PAUL. M. «Internet privacy and the State» en *Connecticut Law Review*, vol. 32, 2000, págs. 815-859 (cit. p. 820)

29 GDT. Recomendación 1/1999, de 23 de febrero, sobre el tratamiento invisible y automático de datos personales en Internet. Doc. 5093/98/ES/final WP 17.pág. 2

30 En la Recomendación 3/97, de 3 de diciembre de 1997, sobre Anonimato en Internet, se planteó -como su título indica, el anonimato como solución de modo que los datos transaccionales generados por la navegación no pudieran asociarse a una persona concreta. En lo que la Recomendación define como navegación pasiva por emplazamientos de Internet de la World Wide Web, que es aquella que genera cookies y archivos data-log, el GDT es muy claro:

«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»

GDT. Recomendación 3/97, de 3 de diciembre de 1997, sobre Anonimato en Internet. Doc. XV D/5022/97 ES final WP 6, pág. 4 y 10.

El Documento de Trabajo sobre Privacidad en Internet añade a esta recomendación una amplia descripción de la panoplia de medios técnicos que podrían contribuir a garantizar el anonimato en la navegación y especialmente recursos como Anonymizer (http://www.anonymizer.com) Zero Knowledge System (http://www.zeroknowledge.com), privada.com o iPrivacy (http://www.iprivacy.com).

GdT. Documento de Trabajo, de 21 de noviembre de 2000, Privacidad en Internet… cit. Pág. 89 y ss.

31 GDT. *Recomendación 17 de mayo de 2001 sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea*. Doc. 5020/01/ES/Final WP 43.

32 GDT. *Recomendación 17 de mayo de 2001*... cit. pág. 7

33 Ibidem, pág. 8.

34 GDT. *Dictamen 2/2002 30 de mayo de 2002 sobre el uso de identificadores únicos en los equipos terminales de telecomunicaciones: ejemplo del IPv6*. Doc. 10750/02/ES/Final WP 58, págs. 6 y 7.

35 GDT. Dictamen 2/2002 30 de mayo de 2002 sobre el uso de identificadores únicos en los equipos terminales de telecomunicaciones: ejemplo del IPv6. Doc. 10750/02/ES/Final WP 58, págs. 6 y 7.

36 El Grupo de trabajo ha subrayado la necesidad de tener en cuenta la necesidad y condiciones de un identificador único en los servicios de autentificación online.

GdT. Documento de trabajo de 2 de julio de 2002. Primeras orientaciones del Grupo de Trabajo del artículo 29 sobre los servicios de autenticación en línea. Doc. núm. 11203/02/ES/Final WP 60.

37 Y precisa « El fundamento jurídico deberá definir precisamente los límites y modalidades de su ejercicio, por medio de normas claras y detalladas, necesarias sobre todo debido al perfeccionamiento continuo de los medios técnicos utilizables. Este texto legal debe ser accesible al público para que el ciudadano pueda prever las consecuencias de su comportamiento».

GDT. *Recomendación 2/1999, de 3 de mayo, sobre la protección de la intimidad en el contexto de la interceptación de las telecomunicaciones*. Doc 5005/99/def. WP 18, pág. 5.

No resulta extraño por tanto que el GdT haya suscrito la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones. En ella se opina sobre las propuestas de retener datos de tráfico durante al menos una año, planteadas en el marco del Tercer Pilar. En tal sentido subrayan que «debe haber una necesidad demostrable, el período de retención debe ser tan corto como sea posible y la práctica debe estar claramente regulada por la ley, de manera que proporcione suficientes salvaguardias frente a un acceso ilegal o cualquier otro abuso. Una retención sistemática de todas las clases de datos de tráfico para un período de un año o más sería claramente desproporcionada y, por lo tanto, inaceptable en todo caso».

Gdt. Dictamen 5/2002, sobre la Declaración de los Comisarios Europeos responsables de protección de datos en la Conferencia Internacional celebrada en Cardiff (9-11 de septiembre de 2002) sobre la retención sistemática obligatoria de datos sobre tráfico de telecomunicaciones. Doc. núm. 11818/02/ES/Final WP 64.

38 *Ibidem,* pág. 7.

39 En coherencia con sus planteamientos El GdT, en el contexto de la lucha contra el ciberdelito, ha subrayado la necesidad de tratar los datos de tráfico de acuerdo con el principio de proporcionalidad. En este sentido se declara que:

«cuando las autoridades encargadas del cumplimiento de la ley estén autorizadas a consultar los datos relativos a las conexiones de una persona en poder de los proveedores de acceso a Internet, dichas autoridades sólo deberían poder tratar los datos de conexión relacionados con la investigación sobre un comportamiento específico (por ejemplo, se deberían poder tratar los datos de conexión relativos a una intrusión ilícita en la Intranet de una empresa, pero no los datos relativos a las costumbres de navegación del autor de la intrusión que no tengan relación con la infracción investigada). De la misma forma, el hecho de que los individuos dejen señales de su presencia en las redes y de que se conserven sus datos personales (a veces sin que la persona interesada lo sepa) no implica que todos estos datos puedan utilizarse automáticamente para una investigación concreta. De manera más general, el Grupo es consciente de que, a la hora de incautarse de datos informáticos, puede ser difícil determinar directamente cuáles son los datos pertinentes y los que no lo son, pero, encualquier caso, es fundamental que sólo se conserven los primeros».

GdT. Dictamen 9/2001, de 5 de noviembre de 2001, sobre la comunicación de la Comisión titulada «Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos». Doc. núm. 5074/01/ES/final WP 51, pag. 5.

En este documento, además de reiterar los principios comunes que ha ido decantando la jurisprudencia del TEDH, -previsión normativa, necesidad social imperiosa, proporcionalidad en el doble sentido de idoneidad e intervención lesiva mínima, limitación temporal de la medida, especificación de su contenido y alcance subjetivo, objetivo y temporal, motivación y adopción por la autoridad competente según el Ordenamiento nacional y derecho a un recurso judicial–, añade alguna consideración específica a tener en cuenta:

«- para los casos en los que se obtengan datos que no sean pertinentes (datos relativos a terceros, datos no pertinentes para la infracción investigada, etc.) mediante las medidas procesales, deberían establecerse garantías específicas y, concretamente, medidas de borrado de tales datos;

- debería contemplarse la posibilidad de informar a la persona afectada sobre la aplicación de la medida procesal a partir del momento en que tal información no perjudique o deje de perjudicar a la investigación;

- debería aplicarse de manera efectiva la transparencia democrática de las medidas procesales, por ejemplo, mediante la elaboración de informes sobre política delictiva;

- la aplicación de la medida debe ser objeto de autorización por parte de una autoridad judicial o equivalente con competencias en la materia y sometida a un control independiente;»

Ibídem pág. 6.

40 GDT. Recomendación 3/99, de 7 de septiembre, sobre la conservación de los datos sobre tráfico por los proveedores de servicio de Internet a e efectos del cumplimiento de la legislación. Doc. 5058/99/ES/FINAL WP 25.

41 En concreto el Grupo de Trabajo ha señalado:

«En vista de lo anterior, el Grupo considera que los medios más eficaces para evitar riesgos inaceptables a la intimidad y reconocer simultáneamente la necesidad de una ejecución eficaz de la ley es que, en principio, los datos sobre tráfico no deberán conservarse a efectos exclusivos de control y que las legislaciones nacionales no deberán obligar a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicios Internet a conservar los datos sobre tráfico durante un plazo superior al necesario a efectos de facturación.

El Grupo recomienda que la Comisión Europea proponga medidas apropiadas para una mayor armonización del plazo durante el cual se permite a los operadores de telecomunicaciones, proveedores de servicios de telecomunicación y proveedores de servicio Internet conservar los datos sobre tráfico para facturación y pago de interconexiones. El Grupo considera que este plazo deberá ser suficiente para permitir a los consumidores impugnar la factura, pero lo más breve posible para no sobrecargar a los operadores y proveedores de servicios y para respetar los principios de proporcionalidad y especificidad como componentes del derecho a la intimidad. Este plazo debe ser conforme con los mayores niveles de protección observados en los Estados miembros. El Grupo llama la atención sobre el hecho de que en varios Estados miembros se han aplicado satisfactoriamente plazos no superiores a tres meses.

Por último, el Grupo recomienda que los gobiernos nacionales tengan en cuenta estas consideraciones».

GDT. *Recomendación 3/99*..., cit. pág. 7.

Debe subrayarse que la posición del GdT en esta materia se mantiene a lo largo del tiempo con pocas variaciones, como puede colegirse de los distintos informes citados en este trabajo. Asimismo, parece evidente que se trata de una cuestión que preocupa profundamente. Sólo así puede entenderse la emisión de un nuevo documento en el que se sintetiza su posición con motivo de la propuesta por 4 Estados miembros de medidas específicas en este campo. Véase GdT. Avis 9/2004 sur le projet de décision cadre sur la conservation de données traitées et stockées en relation avec la mise à disposition de services de communications électroniques disponibles publiquement ou de données sur les réseaux de communications publiques aux fins de la prévention, l'étude, la détection et la poursuite des actes criminels, y compris le terrorisme. [proposition présentée par la France, l'Irlande, la Suède et la Grande-Bretagne (Document du Conseil 8958/04 du 28 avril 2004)] Doc. núm. 11885/04/FR WP 99.

42 Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas o Directiva sobre la privacidad y las comunicaciones electrónicas (DOCE, Serie L, núm. 201 de 31 de julio).

43 Por ejemplo, uno de los métodos utilizados por las productoras cinematográficas estadounidenses para rastrear posibles infracciones a los derechos de propiedad intelectual en internet consiste en instalar y utilizar programas peer to peer, -como eMule o Kazaa-, y buscar a usuarios que distribuyan sus productos. Una vez iniciada la descarga de ficheros, a través de uno o varios usuarios la productora obtiene su número IP. Como se recordará el número IP identifica la red de procedencia del ordenador. Pues bien, una vez identificado el dominio, por ejemplo de una universidad española, la empresa requiere

44 Esta cuestión excede con mucho el objeto de este trabajo véase MARTÍNEZ MARTÍNEZ, RICARD. «Vida privada en Internet (II). La monitorización informática» en *Revista datos personales.org, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 8, marzo de 2004. Disponible en http://www.madrid.org/comun/datospersonales/0,3126,457237_0_460419_12190402_12173401,00.html.

45 Esta cuestión ha sido ampliamente debatida en la doctrina norteamericana. Véanse por todos CATE, FRED. H. *Privacy in the Information Age*, Brookings Institution Press, Washington, D.C., 1997. CATE, FRED. H. «Principles on Internet Privacy» en *Connecticut Law Review*, vol. 32, Spring 2000, págs. 877-896 y SCHWARTZ, PAUL. M. «Internet privacy and the State» en *Connecticut Law Review,* vol. 32, Spring 2000.

Véase asimismo el capítulo primero de mi trabajo, *Una aproximación crítica a la autodeterminación informativa*. Madrid, Thomson-Civitas-APDCM, 2004

46 Es un hecho conocido que tras la implantación de chips con programas de gestión en distintos electrodomésticos la nueva generación de productos aporta la conexión a internet como uno de sus elementos estrella. Simplificando mucho puede señalarse la existencia de dos tipos de aparatos: aquellos que podrán administrarse remotamente y aquellos que, o bien podrán utilizarse para conectarse a Internet, o bien se conectarán directamente con la finalidad de transmitir información sobre sus necesidades o las del propietario. El primer paso en esta línea lo están dando los electrodomésticos de gama blanca. En este sentido, en un futuro muy próximo podremos ordenar a nuestra lavadora que se ponga en marcha para que la colada este finalizada al llegar a casa. Ésta podrá administrar aspectos como programa de lavado, temperatura, centrifugado etc,, –gracias al etiquetado de la ropa y sensores de peso–, e incluso comunicarse con la secadora a fin de transmitirle instrucciones precisas. Del mismo modo, este nuevo usuario domotizado iniciará el programa de su microondas mediante el teléfono móvil cuando se acerque al domicilio, o lo detendrá si sufre un atasco. Además podrá controlar la temperatura doméstica a distancia, verificar el cuidado que reciben sus hijos o si la empresa de limpieza es diligente gracias a pequeñas webcams. Para finalizar, y el lector puede imaginar miles de posibilidades adicionales, el frigorífico podrá componer la lista de la compra, y en su caso la remitirá a la tienda, en función del estado de las existencias y de las preferencias del usuario. Como resulta evidente, el simple acceso al tráfico generado por las IP de estos aparatos ofrecerá datos sustanciales tanto a los fabricantes de electrodomésticos como a toda la cadena de establecimientos vinculados a la economía doméstica.

El entorno físico en el que se producirá este fenómeno, se ha denominado residencia virtual. Por otra parte, estos dispositivos permitirán la generación de lo que se ha dado en llamar "entorno de Inteligencia Ambiental total" (Aml) que, en palabras del IPTS, «será capaz de reconocer y adaptarse a la presencia de diferentes individuos trabajando sin discontinuidades, sin obstrucciones y a menudo de forma invisible.

INSTITUTE FOR PROSPECTIVE TECHMOLOGICAL STUDIES. *Seguridad y privacidad para el ciudadano en la era digital posterior al 11 de septiembre: una visión prospectiva*. Resumen ejecutivo. Comisión Europea, julio 2003, pág. 10.

47 cita trabajo del IST

48 CASTELLS, MANUEL. *La Galaxia Internet*. Areté, Barcelona, 2001.

49 En Internet se manifiesta con claridad la dimensión informacional de la vida privada ya que su funcionamiento se basa esencialmente en el intercambio, transferencia y acumulación de información. Como se ha visto, la posibilidad de procesar informaciones a partir de datos personales más o menos voluntariamente cedidos permite que el usuario revele de modo inconsciente hábitos, gustos, preferencias, ideología etc.

Véase, POULLET, YVES. «Internet et vie privée» en VV.AA. *Società dell'informazione. Tutela della riservatezza*. Collana dell'Osservatorio Giordano dell'Amore sui rapporti tra Diritto ed Economia. Giuffré, Milano, 1998, págs. 49-72.

50 A este respecto, el Tribunal Constitucional en el fundamento jurídico 3.º de su STC 110/1984 señala: «El reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española. Pero su idea originaria, que es el respeto a la vida privada, aparece ya en algunas de las libertades tradicionales. La inviolabilidad de domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado. Lo ocurrido es que el avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de

conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad».

51 Para el profesor Espín Templado la vida privada se define como «el conjunto de circunstancias y datos relativos a la vida de una persona que quedan fuera del conocimiento de los demás, salvo que medie un expreso deseo de comunicarlo o de ponerlo de manifiesto por parte de la persona afectada, y al margen naturalmente, de las personas que compartan con ella aspectos más o menos amplios de su vida. Todos esos datos, que quedan comprendidos dentro de la vida privada de una persona constituyen gran parte de sus actividades y en modo alguno versan necesariamente sobre aspectos íntimos de su vida». Por tanto este planteamiento se formula con vocación de alcanzar a las repercusiones en el derecho a la intimidad derivadas del uso de las tecnologías de la información. Espín Templado, Eduardo. «Fundamento y alcance del derecho fundamental a la inviolabilidad del domicilio», en *Revista del centro de Estudios Constitucionales*, nº 8. Enero - abril 1991, págs. 45-46.

Véase así mismo Ruiz Miguel, Carlos. «En torno a la protección de los datos personales automatizados». *Revista de Estudios Políticos* (Nueva Época), núm. 84 abril-junio 1994 y Ruiz Miguel, Carlos, *La Configuración Constitucional del Derecho a la Intimidad.* Tecnos, Madrid, 1995, y Ruiz Miguel, Carlos. «En torno a la protección de los datos personales automatizados». *Revista de Estudios Políticos* (Nueva Época), núm. 84 abril-junio 1994.

52 Véase por todas la STC 292/2000.

53 Véase la extensa obra de Pablo Lucas Murillo de la Cueva

- «La protección de los datos personales ante el uso de la informática», en VV. AA., *Diez años de desarrollo constitucional Estudios en homenaje al Profesor Don Luis Sánchez Agesta.* Universidad Complutense, Madrid, 1989.

- *El derecho a la autodeterminación informativa.* Tecnos, Temas clave, Madrid, 1990.

- *Informática y protección de datos personales (estudios sobre la Ley Orgánica 5/1992 de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal).* Cuadernos y Debates. Centro de Estudios Constitucionales, Madrid, 1993.

- «La construcción del derecho a la autodeterminación informativa» en *Revista de Estudios Políticos*, Nueva Época, núm. 104, abril-junio 1999 y Lucas Murillo de la Cueva, Pablo. «La primera jurisprudencia sobre el derecho a la autodeterminación informativa», en *Datos Personales, Revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, núm. 1, Marzo 2003. Disponible en http://www.comadrid.es/comun/datospersonales/0,3126,457237_458332_460269_12039319_0,00.html

54 Esto en la práctica obliga al usuario a mentir a la menor ocasión, lo que conduce a su vez a situaciones bastante absurdas y, llevadas al extremo, perniciosas para la tutela de la vida privada. Así, multitud de portales ofrecen espacios gratuitos para la ubicación de páginas Web sujetos a modelos de contrato en los que el proveedor se autoexime de cualquier responsabilidad. Puesto que aún no parece haberse generalizado, ni tampoco exigirse, el empleo de firmas o certificados digitales que adveren la identidad de los futuros clientes, el internauta puede fingir una identidad sin más exigencia que la de que el número del NIF y su letra de control sean coherentes. Además, no es infrecuente toparse con páginas con contenidos ilícitos, nocivos o atentatorios contra el honor o la vida privada de los ciudadanos o, simplemente dedicadas a la recolección de datos, esencialmente direcciones de correo electrónico, sin ningún tipo de respeto a la legalidad vigente.

55 Ello sin contar con aquellos casos en los que el usuario se ve constreñido a aceptar un contrato de uso ilegible tanto en términos semánticos como incluso físicos. Es conocido com en internet se acude a triquiñuelas como editar la información legal con un tamaño de letra ilegible y mediante la presentación en desplegables de una amplitud irrisoria, que sólo editan una línea cada vez y resultan profundamente incómodos al ojo y la paciencia humanos.

Véase Martínez Martínez, Ricard.«Vida privada en Internet»…*Op. Cit.* Y Martínez Martínez, Ricard. «Vida privada en Internet (II). La monitorización informática», *Op. Cit.*

56 Véase, Martín Morales, Ricardo. *El régimen constitucional del secreto de las comunicaciones*. Civitas, Madrid, 1995 y Rodríguez Ruiz, Blanca. *El secreto de las comunicaciones: tecnología e intimidad*. McGraw Hill, Madrid, 1998.

57 La sentencia tenía su origen en el empleo de la grabación fonográfica como prueba para legitimar un despido. STC 114/1984

58, El Tribunal Constitucional ha incorporado los principios definidos por el Tribunal Europeo de Derechos Humanos en aplicación del artículo 8 CEDH y manifestado en los asuntos como Klass, Malone, Kruslin y, en lo que a España se refiere en el asunto Valenzuela Contreras.

La mayoría de sus sentencias se refiere a la práctica de interceptaciones de las comunicaciones judicialmente autorizadas y se estudia la posible vulneración del artículo 18.3 CE en relación con los derechos del artículo 24 CE y en la exigencia de declaración de la nulidad de la prueba. Sobre las condiciones procesales asociadas a la autorización judicial de la interceptación de las comunicaciones véanse las SSTC 85/1994, 86/1995, 181/1995, 170/1996, 151/1998 y 171/1999. En la misma línea argumental, pero con expresa referencia a la jurisprudencia del Tribunal Europeo de Derechos Humanos cabe citar las STC 49/1996, 54/1996, 127/1996, 49/1999, 141/1999, 14/2000 y 138/2001

Véase, RIVES SEVA, ANTONIO PABLO. *La intervención de las comunicaciones en la jurisprudencia penal*. Aranzadi, Pamplona, 2000 y RODRÍGUEZ LAINZ, JOSÉ LUÍS. *Intervención judicial en los datos de tráfico de las telecomunicaciones*. Bosch, Barcelona, 2003.

Por otra parte, las exigencias que debe satisfacer la interceptación de las comunicaciones en los supuestos de lucha antiterrorista se definen en la STC 199/1987 sobre los Recursos de inconstitucionalidad interpuestos por el Parlamento de Cataluña y el Parlamento del País Vasco frente a la LO 9/1984, de 26-12-1984, de medidas contra la actuación de bandas armadas y elementos terroristas y de desarrollo del art. 55, párr. 2º de la Constitución.

59 Postura que se reitera en sede de inviolabilidad del domicilio en el fundamento jurídico séptimo de la STC 94/1999.

60 Así:

«6. La aplicación de la doctrina expuesta conduce a concluir que la entrega de los listados por las compañías telefónicas a la policía sin consentimiento del titular del teléfono requiere resolución judicial, pues la forma de obtención de los datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE. En efecto, los listados telefónicos incorporan datos relativos al teléfono de destino, el momento en que se efectúa la comunicación y a su duración, para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras está teniendo lugar, con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso a efectos, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión. Dichos datos configuran el proceso de comunicación en su vertiente externa y son confidenciales, es decir, reservados del conocimiento público y general, además de pertenecientes a la propia esfera privada de los comunicantes. El destino, el momento y la duración de una comunicación telefónica, o de una comunicación a la que se accede mediante las señales telefónicas, constituyen datos que configuran externamente un hecho que, además de carácter privado, puede asimismo poseer un carácter íntimo.

Ahora bien, aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las "escuchas telefónicas", siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad.

Hemos de separarnos, pues, de la argumentación desarrollada por el Juzgado de lo Penal y la Audiencia Provincial en las decisiones impugnadas, ya que la entrega de los listados a la policía afecta al objeto de protección del derecho fundamental al secreto de las comunicaciones, aunque ello no signifique, como se razonará a continuación, que se haya ocasionado en este caso la vulneración de este derecho fundamental».

61 En este campo, como en tantos otros, se aprecia la existencia de una suerte de tensión normativa, o de conflictividad latente. Ya se visto al citar la Consulta 1/1999, hasta que punto las comunicaciones de datos previstas por el art. 11.2 LOPD entraban en conflicto con la Ley General de Telecomunicaciones y la Ley de Enjuiciamiento Criminal. Si se considera que el número IP forma parte, por decir de algún modo, “estructural” de las comunicaciones en Internet se requerirá el cumplimiento de la garantía judicial a la que se refiere el art. 18. 3CE. Un conflicto parecido parece apuntar

Rodríguez Lainz entre el régimen previsto por la Ley 34/2002, de 11 de julio, de servicios de sociedad de la información y de comercio electrónico y la LOPD. En su opinión las obligaciones impuestas a los ISP por la primera vendrían a justificar que estos pusieran de motu proprio en conocimiento de los tribunales o del Ministerio Fiscal la existencias de comportamientos delictivos deducibles de su tráfico de internet. Sin embargo, el deber de secreto del art. 10 LOPD entraría en contradicción con ello. En cualquier caso, y como se ha apuntado en el texto el autor entiende que deberá contarse con el consentimiento del comunicante para tratar ciertos datos ya que de lo contrario se aplicaría el régimen general del secreto de las comunicaciones.

RODRÍGUEZ LAINZ, JOSÉ LUÍS. *Intervención judicial…, op. cit.* págs. 136 y ss.

62 Fernández Rodríguez distingue dentro de lo que denomina servicios de Red, los servicios de comunicación propiamente dicha, los de acceso a la información y los búsqueda de información. FERNÁNDEZ RODRÍGUEZ, JOSÉ LUÍS. *Secreto e intervención de las comunicaciones en internet*. Thomson-Civitas-APDCM, Madrid, 2004, pp. 46 y ss.