I

*(Resoluciones, recomendaciones y dictámenes)*

# DICTÁMENES

# SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

## Dictamen del Supervisor Europeo de Protección de Datos sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales

(2012/C 34/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado de Funcionamiento de la Unión Europea y, en particular, el artículo 16,

Vista la Carta de los Derechos Fundamentales de la Unión Europea y, en particular, sus artículos 7 y 8,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [1],

Visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [2], y en particular el artículo 41, apartado 2,

Vista la 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 [3].

HA ADOPTADO EL SIGUIENTE DICTAMEN:

### I. **INTRODUCCIÓN**

#### I.1. **Antecedentes**

1. El 19 de abril de 2011, la Comisión adoptó una Comunicación relativa al internet abierto y la neutralidad de la red en Europa [4].

2. El presente dictamen puede considerarse como la reacción del SEPD a dicha Comunicación y tiene por objeto contribuir al debate de las políticas de la UE en curso sobre neutralidad de la red, especialmente sobre los aspectos relacionados con la protección de datos y la intimidad.

---

[1] DO L 281 de 23.11.1995, p. 31, la «Directiva sobre protección de datos».
[2] DO L 8 de 12.1.2001, p. 1, el «Reglamento sobre protección de datos».
[3] DO L 201 de 31.7.2002, p. 37, modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (véase la nota al pie de página nº 15), la «Directiva sobre la privacidad y las comunicaciones electrónicas».
[4] COM(2011) 222 final.

3. El dictamen se elabora sobre la base de la respuesta ([5]) del SEPD a la consulta pública de la Comisión sobre la internet abierta y la neutralidad de la red en Europa, que precedió a la Comunicación de la Comisión. El SEPD también ha considerado el reciente proyecto de conclusiones del Consejo sobre neutralidad de la red ([6]).

### I.2. **El concepto de neutralidad de la red**

4. La neutralidad de la red hace referencia a un debate en curso sobre si debe permitirse a los proveedores de servicios de internet [«PSI ([7])»] que limiten, filtren o bloqueen el acceso a internet o que puedan afectar de otro modo su funcionamiento. El concepto de neutralidad de la red se basa en la idea de que la información en internet partout dans le document, s.v.p debe ser transmitida con imparcialidad, sin tener en cuenta el contenido, el destino o el origen, y que los usuarios deberían poder decidir qué aplicaciones, servicios y hardware desean utilizar. Esto significa que los PSI no pueden, a su elección, dar prioridad o ralentizar el acceso a determinadas aplicaciones o servicios como los de igual a igual («P2P»), etc ([8]).

5. El filtrado, el bloqueo y la inspección del tráfico de la red plantea cuestiones importantes, que con frecuencia pasan desapercibidas o están marginadas, en relación con la confidencialidad de las comunicaciones y el respeto de la intimidad de las personas y de sus datos personales cuando utilizan internet. Por ejemplo, determinadas técnicas de inspección implican la vigilancia del contenido de las comunicaciones, los sitios web visitados, los correos electrónicos enviados y recibidos, el momento en que esto tiene lugar, etc., permitiendo el filtrado de las comunicaciones.

6. Al inspeccionar los datos de las comunicaciones, los PSI pueden vulnerar la confidencialidad de las comunicaciones, derecho fundamental garantizado por el artículo 8 del Convenio Europeo de Derechos Humanos (el «CEDH») y los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (la «Carta»). La confidencialidad está además protegida en la legislación secundaria de la Unión Europea, en particular en el artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas.

### I.3. **Objeto y estructura del dictamen**

7. El SEPD considera que un debate político serio sobre la neutralidad de la red debe tratar la confidencialidad de las comunicaciones, así como otras implicaciones relativas a la protección de datos y a la intimidad.

8. El presente dictamen contribuye a este debate en curso de la Unión Europea. El objetivo del mismo es triple:

   — remarca la relevancia de la intimidad y la protección de datos en los actuales debates sobre la neutralidad de la red. De modo más particular, resalta la necesidad de respetar las normas existentes sobre confidencialidad de las comunicaciones. Deberían permitirse únicamente las prácticas que respeten dichas normas,

   — la neutralidad de la red hace referencia a las posibilidades — tecnológicas — relativamente nuevas y hay poca experiencia sobre cómo se aplica el marco jurídico. Por tanto, el dictamen ofrece orientaciones sobre el modo en que los PSI deben aplicar y respetar el marco jurídico de protección de datos si se implican en el filtrado, el bloqueo y la inspección del tráfico de red. Esto debería ser útil tanto para los PSI como para las autoridades encargadas de controlar la aplicación del marco,

   — dentro del ámbito de protección de datos y de la intimidad, el presente dictamen identifica ámbitos que requieren una atención especial y que pueden exigir acciones a escala de la Unión Europea. Esto es especialmente importante a la luz del debate en curso a escala de la Unión Europea y las medidas políticas que la Comisión puede iniciar en este contexto.

([5]) El SEPD respondió destacando la importancia de tener en cuenta las cuestiones de protección de datos e intimidad, junto con otros derechos y valores existentes. La respuesta está disponible en: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf

([6]) Disponible en http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf

([7]) Esto incluye el suministro tanto de acceso fijo como móvil a internet.

([8]) Aunque el principio no es aplicable a que los PSI pongan límites en relación con la velocidad o la cantidad de información que el abonado puede enviar o recibir a través de abonos con límites de ancho de banda o de volumen. Por tanto, en virtud del principio de neutralidad de la red, los PSI todavía podrían ofrecer abonos de acceso a internet que limitan el acceso sobre la base de criterios como la velocidad o el volumen, siempre y cuando no se exija discriminar a favor o en contra de determinado contenido.

9. El SEPD es consciente de que la neutralidad de la red plantea otras cuestiones, que se describen posteriormente, tales como las relacionadas con el acceso a la información. Estas cuestiones únicamente se tratan en la medida en que estén relacionadas o tengan un impacto sobre la protección de datos y la intimidad.

10. El dictamen está estructurado de la siguiente manera. El apartado II comienza proporcionando una breve visión general de las prácticas de filtrado por parte de los PSI. El apartado III destaca el marco jurídico de la Unión Europea sobre neutralidad de la red. El apartado IV continúa con una descripción técnica seguida de una evaluación de las repercusiones sobre la intimidad, en función de la técnica que se utilice. El apartado V analiza los detalles prácticos relacionados con la aplicación del actual marco de la protección de datos y la intimidad de la Unión Europea. Sobre la base del análisis, el apartado VI incluye sugerencias para otras medidas políticas e identifica los ámbitos en que podría ser necesario aclarar y mejorar el marco jurídico. El apartado VII incluye las conclusiones.

## II. **POLÍTICAS DE NEUTRALIDAD DE LA RED Y GESTIÓN DEL TRÁFICO**

*Uso creciente de las políticas de gestión del tráfico*

11. Tradicionalmente, los PSI han controlado e influido en el tráfico de la red únicamente en circunstancias limitadas. Por ejemplo, los PSI han aplicado técnicas de inspección y flujos de información limitados para preservar la seguridad de la red, por ejemplo, para combatir los virus. Por ello, en general, internet ha crecido manteniendo, sin embargo, un alto grado de neutralidad.

12. Sin embargo, en los últimos años, algunos PSI han mostrado interés en inspeccionar el tráfico en la red para diferenciar y aplicar distintas políticas al mismo, por ejemplo, para bloquear servicios específicos o dar preferencia de acceso a otras personas. A esto se le conoce a veces con la denominación de «políticas de gestión del tráfico» ([9]).

13. Son muchos los motivos por los que los PSI inspeccionan y diferencian el tráfico. Por ejemplo, las políticas de gestión del tráfico pueden ayudar a los PSI a gestionar el tráfico durante períodos altamente congestionados, por ejemplo, dando prioridad a un determinado tráfico para el que el factor del tiempo es importante, como el flujo continuo de vídeo y bajando de categoría otros tipos de tráfico para los que el factor del tiempo no sea importante, como los servicios de igual a igual ([10]). Además, la gestión del tráfico puede ser un medio para que los PSI obtengan un potencial flujo de ingresos, cuyo origen puede estar en distintas fuentes. Por un lado, los PSI podrían cobrar cuotas a los proveedores de servicios de contenido, por ejemplo, aquellos cuyos servicios exijan el uso de un mayor ancho de banda, a cambio de darles prioridad (y, por ende, velocidad). Esto implicaría que el acceso a un determinado servicio, por ejemplo, un servicio que proporcione vídeos a la carta, sería más rápido que acceder a otro servicio similar que no ha contratado una transmisión de alta velocidad. También podrían obtenerse ingresos de los abonados interesados en pagar cuotas más altas (o más bajas) para determinados tipos de abonos diferenciados. Por ejemplo, un abono sin acceso a servicios P2P podría ser más barato que otro que ofrezca un acceso ilimitado.

14. Además de que los motivos propios del PSI para el uso de políticas de gestión del tráfico, otras partes también pueden tener un interés en que el proveedor utilice dichas políticas. Si el PSI gestiona sus redes y lleva a cabo una inspección del contenido que se desarrolla mediante sus servicios, es posible que aumente su capacidad de detectar supuestos usos ilícitos, por ejemplo, la vulneración de los derechos de autor o un uso pornográfico.

([9]) Véase por ejemplo el Informe de OFCOM titulado «Site blocking to reduce online copyright infringement» (Bloqueo de sitios para reducir la vulneración en línea de los derechos de autor), adoptado el 27 de mayo de 2011, disponible en: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: «Some ISPs already deploy packet inspection systems in their network for traffic management and other purposes, so we assume that it can be deployed, albeit that this would involve a high level of complexity and cost for those not already running such services. It may be that in the short to medium term DPI could only be deployed by the larger ISPs given the capital investment required (Algunos PSI ya implantan sistemas de inspección de paquetes en su red para la gestión del tráfico y otros fines, por ello asumimos que pueden ser implantados, aunque ello implicaría un alto nivel de complejidad y coste para quienes no tengan en funcionamiento dichos servicios. Teniendo en cuenta la inversión de capital que es necesaria, es posible que a corto y a medio plazo únicamente los grandes PSI puedan implantar la inspección profunda de paquetes)».

([10]) La calidad de las aplicaciones en tiempo real como el flujo continuo de vídeo depende, entre otras cosas, de la latencia, es decir, del retraso debido, por ejemplo, a la congestión de la red.

*Otros intereses en juego, incluidas la protección de datos y la intimidad*

15. Esta tendencia ha dado lugar a un debate sobre la legitimidad de este tipo de prácticas y, más concretamente, sobre si deberían establecerse legalmente obligaciones específicas de neutralidad en la red.

16. El uso creciente de las políticas de gestión del tráfico por parte de los PSI posiblemente podría limitar el acceso a la información. Si esta conducta se convierte en una práctica común y a los usuarios no les resulta posible (o les resulta muy caro) disponer de un acceso pleno a internet tal como lo conocemos hoy en día, esto comprometería el acceso a la información y la capacidad del usuario de enviar y recibir el contenido que desee mediante las aplicaciones y los servicios de su elección. Un principio jurídicamente vinculante relativo a la neutralidad de la red puede evitar este problema.

17. Esto lleva al SEPD a valorar las implicaciones para la protección de datos y la intimidad cuando los PSI se implican en la gestión del tráfico, más concretamente:

— en los casos en que los PSI tratan datos de tráfico con el único fin de encaminar el flujo de información del remitente al destinatario, normalmente llevan a cabo un tratamiento limitado de datos personales ([11]). Del mismo modo que los servicios postal tratan la información incluida en el sobre de una carta, el PSI trata la información necesaria para encaminar la comunicación hacia el destinatario. Esto no entra en conflicto con los requisitos legales de protección de datos, intimidad y confidencialidad de las comunicaciones,

— sin embargo, cuando el PSI inspecciona datos de la comunicación para diferenciar cada flujo de comunicación y aplicar políticas específicas, que pueden ser desfavorables para las personas, las implicaciones resultan más significativas. Según las circunstancias de cada caso y el tipo de análisis realizado, el tratamiento puede ser altamente intrusivo en los datos personales y la intimidad de las personas. Esto resulta más obvio cuando las políticas de gestión revelan el contenido de las comunicaciones de internet de las personas, incluidos los mensajes de correo electrónico recibidos y enviados, los sitios web visitados, los ficheros descargados o subidos, etc.

## III. **PANORAMA GENERAL DEL MARCO JURÍDICO DE LA UNIÓN EUROPEA SOBRE NEUTRALIDAD DE LA RED Y OTRAS MEDIDAS POLÍTICAS**

### III.1. **El marco jurídico en pocas palabras**

18. Hasta 2009, los instrumentos legislativos de la Unión Europea no incluían disposiciones que prohibieran explícitamente a los PSI llevar a cabo filtrados o bloqueos ni cobrar costes extras a los abonados por el acceso a los servicios. Al mismo tiempo, tampoco incluían disposiciones que reconocieran de modo explícito esta práctica. En cierto modo, era una situación que generaba inseguridad.

19. El Paquete Telecom de 2009 cambió esta situación al incluir disposiciones que favorecían la apertura de internet. Por ejemplo, el artículo 8, apartado 4, del marco regulador común de las redes y los servicios de comunicaciones electrónicas (en adelante, la «Directiva marco») establece la obligación de las autoridades de reglamentación de promover la capacidad de los usuarios finales para acceder al contenido, las aplicaciones o los servicios de su elección ([12]). Esta disposición es aplicable a la red en su conjunto, no a escala de los proveedores individuales. El reciente proyecto de conclusiones del Consejo también destaca la necesidad de mantener la apertura de internet ([13]).

([11]) Esto excluye las operaciones destinadas a aumentar la seguridad de la red y a detectar el tráfico perjudicial así como las operaciones exigidas para la facturación y las interconexiones. También excluye las obligaciones que derivan de lo dispuesto en la Directiva de conservación de datos, la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios en comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, (DO L 105 de 13.4.2006, p. 54) (en adelante, la «Directiva de conservación de datos»).

([12]) Directiva 2002/21/CE, de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, modificada por la Directiva 2009/140/CE y el Reglamento (CE) nº 544/2009, (DO L 337 de 18.12.2009, p. 37).

([13]) Véase el punto 3, letra e), en el que el Consejo reconoce: «La necesidad de mantener la apertura de internet al mismo tiempo que se garantiza que continuará ofreciendo servicios de gran calidad en un marco que promueve y respeta los derechos fundamentales como la libertad de expresión y la libertad de empresa» y en el punto 8, letra d), en la que invita a los Estados miembros a «promover el carácter abierto y neutral de internet como objetivo de sus políticas».

20. La Directiva de servicio universal ([14]) incluye obligaciones más concretas. Los artículos 20 y 21 establecen exigencias de transparencia respecto de las limitaciones del acceso o el uso de los servicios y aplicaciones, lo cual exige también niveles mínimos de calidad de servicio.

21. En cuanto a las prácticas de los PSI que conlleven la inspección de las comunicaciones de las personas, el considerando 28 de la Directiva por la que se modifica las Directivas de servicio universal y sobre privacidad ([15]) destaca que «en función de la tecnología que se utilice y del tipo de limitación, dichas limitaciones pueden requerir el consentimiento del usuario en virtud de la Directiva sobre la privacidad y las comunicaciones electrónicas». De este modo, el considerando 28 recuerda la necesidad de consentimiento en virtud de lo dispuesto en el artículo 5, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas para cualquier limitación basada en la vigilancia de las comunicaciones. El apartado IV analiza con más detalle la aplicación del artículo 5, apartado 1, y el marco jurídico general de la protección de datos y la intimidad.

22. Por último, el artículo 22, apartado 3, de la Directiva de servicio universal ahora faculta a las autoridades nacionales de reglamentación a que, en caso necesario, impongan unos requisitos mínimos de calidad del servicio a los PSI para evitar la degradación del servicio y la obstaculización o ralentización del tráfico en las redes públicas.

23. Lo anterior quiere decir que a escala de la Unión existe una amplia aspiración de que internet sea abierta (véase el artículo 8, apartado 4, de la Directiva marco). Sin embargo, este objetivo político, que se aplica a la red en su conjunto, no está directamente vinculado a las prohibiciones u obligaciones de los PSI individuales. Dicho de otro modo, un PSI puede adoptar políticas de gestión del tráfico que pueden excluir el acceso a determinadas aplicaciones, siempre que los usuarios finales estén totalmente informados y hayan expresado su consentimiento libre, específico e inequívoco.

24. La situación puede ser distinta según cada Estado miembro. En algunos Estados miembros, los PSI pueden, en condiciones específicas, establecer políticas de gestión del tráfico, por ejemplo, para bloquear aplicaciones como las de voz sobre el protocolo internet (VoIP) (como parte de un abono a internet más barato) siempre que las personas hayan prestado su consentimiento informado libre, específico e inequívoco. Otros Estados miembros han optado por reforzar el principio de neutralidad de la red. Por ejemplo, en julio de 2011, el Parlamento neerlandés aprobó una ley que prohibía de manera general que los proveedores obstaculizaran o ralentizaran las aplicaciones o servicios de internet (como los de VoIP), salvo si esto es necesario para minimizar los efectos de la congestión, por razones de integridad o seguridad, para luchar contra el correo no deseado o si lo exige una orden judicial ([16]).

### III.2. **La Comunicación relativa a la neutralidad de la red**

25. En su Comunicación relativa la neutralidad de la red ([17]), la Comisión Europea concluyó que la situación sobre neutralidad de la red es una cuestión que requiere un seguimiento y un mayor análisis. Su política ha venido a denominarse de «esperar a ver» antes de considerar otras medidas reguladoras.

([14]) Directiva 2002/22/CE modificada por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, (DO L 337 de 18.12.2009, p. 11). Compárese también con el artículo 1, apartado 3, que establece que la Directiva no establece ni prohíbe las condiciones, que limiten el acceso o el uso de los servicios y aplicaciones, cuando así lo permita la legislación nacional y de conformidad con la legislación comunitaria, aunque sí establece una obligación de proporcionar información sobre dichas condiciones.

([15]) Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores.

([16]) El texto original en neerlandés de la enmienda puede encontrarse en: https://zoek.officielebekendmakingen.nl/kst-32549-A.html. Los motivos indicados por la prensa para dicha opción política no hacen referencia a las consideraciones en materia de la protección de datos y la intimidad sino a razones vinculadas a garantizar que no se priva de información a los usuarios o que no se les proporciona un acceso limitado a la información. Por lo tanto, parece que dicha enmienda estuvo motivada por algunas cuestiones relativas al acceso a la información.

([17]) Véase la nota a pie de página 4.

26. La comunicación de la Comisión reconoció que cualquier medida y ulteriores medidas reguladoras quedarían sujetas a una evaluación en profundidad en relación con los aspectos de la protección de datos y la intimidad. El proyecto de conclusiones del Consejo también señala las cuestiones de protección de datos y de intimidad en juego ([18]).

27. La cuestión que debe ser valorada desde el punto de vista de la protección de datos y la privacidad es si una política de esperar a ver es suficiente. Mientras que el marco de protección de datos y de intimidad prevé, en este momento, algunas garantías especialmente a través del principio de confidencialidad de las comunicaciones, parece necesario vigilar de cerca el nivel de cumplimiento y emitir orientaciones en relación con varios aspectos que no están especialmente claros. Además, deberían presentarse algunas reflexiones sobre el modo en que el marco podría ser aclarado y posteriormente mejorado, a la luz de los desarrollos tecnológicos. Si la vigilancia revela que el mercado está evolucionando hacia una inspección masiva de las comunicaciones en tiempo real y de las cuestiones relacionadas con el cumplimiento del marco, será necesario adoptar medidas legislativas. En el apartado VI se formularán sugerencias concretas en este sentido.

## IV. **CONOCIMIENTOS TÉCNICOS Y LAS REPERCUSIONES EN MATERIA DE PROTECCIÓN DE DATOS E INTIMIDAD RELACIONADAS**

28. Antes de analizar más profundamente la cuestión, es importante tener una mejor perspectiva de las técnicas de inspección que los PSI pueden utilizar para participar en la gestión del tráfico y sobre cómo esto puede tener un impacto sobre el principio de neutralidad de la red. Las implicaciones relativas a la protección de datos y a la intimidad que se derivan de dichas técnicas varían sustancialmente en función de la técnica o técnicas que se utilicen. Estos conocimientos técnicos son necesarios para entender y aplicar adecuadamente el marco jurídico de la protección de datos descrito en el apartado V. Sin embargo, cabe señalar que éste es un ámbito complejo y en continuo cambio. Por ello, la descripción que se indica a continuación no pretende ser exhaustiva ni estar totalmente actualizada sino que únicamente ofrece la información técnica que es indispensable para entender el razonamiento jurídico.

### IV.1. **Transmisión de información a través de internet: nociones básicas**

29. Cuando un usuario transmite una comunicación a través de internet, la información transmitida se divide en paquetes. Estos paquetes se transmiten a través de internet desde el remitente al destinatario. Cada paquete incluirá, entre otros, información sobre el origen y el destino. Además, los PSI pueden incluir estos paquetes en otras capas y protocolos ([19]), que se utilizarán para gestionar los distintos flujos de tráfico en la red del PSI.

30. Volviendo a la analogía de la carta postal, utilizar un protocolo de transmisión de red es equivalente a incluir el contenido de la carta en un sobre con una dirección de destino que pueda ser leída por el servicio postal y que éste pueda luego entregar. El servicio postal podrá utilizar protocolos adicionales en sus trámites internos para gestionar todos los sobres que deben transmitirse, siendo el objetivo que cada sobre llegue a su destino, tal como el remitente indicó en el origen. Siguiendo la analogía, cada paquete tiene dos partes, la carga útil IP (*IP payload*) que incluye el contenido de la comunicación y será equivalente a la carta. Contiene información únicamente dirigida al destinatario. La segunda parte del paquete es la cabecera de IP (*IP header*) que incluye, entre otros, la dirección del destinatario y del remitente y es equivalente al sobre. La cabecera de IP permite a los PSI y a otros intermediarios encaminar la carga útil desde la dirección de origen a la dirección de destino.

31. Los PSI y otros intermediarios garantizan que los paquetes IP viajan a través de la red mediante nodos que leen la información de la cabecera de IP, lo comparan con las tablas de encaminamiento y luego las envían hacia el siguiente nodo, de camino a su destino. Este proceso se lleva a cabo a través de la red

([18]) Véase el punto 4, letra e), en el que el Consejo señala: «La existencia de algunas preocupaciones, que derivan principalmente de los consumidores y las autoridades encargadas de la protección de datos, por lo que se refiere a la protección de datos personales».

([19]) Como se describe con más detalle en el apartado IV.2, estos protocolos codifican la información que se transmite de extremo a extremo de la forma acordada, como el HTTP, FTP, etc., de modo que las partes implicadas en la comunicación puedan entenderse entre sí.

utilizando un enfoque «mejor esfuerzo sin memoria» ya que todos los paquetes que llegan a un nodo son tratados de una forma neutral. Cuando se envían al siguiente nodo, no hay necesidad de conservar más información en el encaminador ([20]).

### IV.2. **Técnicas de inspección**

32. Tal como se ha ilustrado anteriormente, los PSI leen las cabeceras de IP con el fin de encaminarlos hacia su destino. Sin embargo, como se ha destacado anteriormente, el análisis del tráfico (que implica cabeceras de IP y cargas útiles de IP) puede realizarse para otros fines y con distintos tipos de tecnologías. Las nuevas tendencias pueden incluir, por ejemplo, la ralentización de determinadas aplicaciones que los usuarios utilizan, como la tecnología P2P, o de modo alternativo, mejorar la velocidad del tráfico para determinados servicios como los servicios de vídeo a la carta para los abonados preferentes. Aunque todas las técnicas de inspección *técnicamente* realizan una inspección de paquetes, estas técnicas suponen distintos niveles de intrusión. Existen dos tipos de categorías principales de técnicas de inspección. Una está basada sólo en la cabecera de IP y la otra incluye también la carga útil de IP.

*Basada en la información de la cabecera de IP*. La inspección de un paquete de cabecera de IP revela algunos campos que pueden permitir a los PSI aplicar una serie de políticas específicas para gestionar el tráfico. Estas técnicas basadas únicamente en la inspección de cabeceras de IP tratan datos que, en principio, están destinados a encaminar información, para un fin distinto (es decir, para diferenciar el tráfico). Mirando la dirección IP de origen, el PSI puede vincularla a un determinado abonado y aplicar algunas políticas específicas, por ejemplo, encaminar el paquete a través de un enlace más rápido o más lento. Mirando la dirección IP de destino, el PSI también puede aplicar políticas específicas, por ejemplo, bloquear o filtrar el acceso a determinados sitios web.

*Basada en una inspección más profunda*. Una inspección profunda de paquetes permite al PSI acceder a la información dirigida únicamente al destinatario de la comunicación. Volviendo al ejemplo del servicio postal, este enfoque es equivalente a abrir el sobre y leer la carta del interior para realizar un análisis del contenido de la comunicación (encapsulado dentro de los paquetes IP) para aplicar una política de red específica. Existen distintos modos de llevar a cabo la inspección, cada uno de los cuales implica distintas amenazas para el interesado.

— *Inspección profunda de paquetes basada en el análisis de los protocolos y en los registros estadísticos.* Además del protocolo de IP, que tiene como fin permitir que los datos se transmitan a través de internet, existen otros protocolos que codifican la información que va a ser transmitida de un modo acordado (transporte, sesión, presentación y aplicación, etc.). El objetivo de estos protocolos es garantizar que las partes implicadas en la comunicación puedan entenderse entre sí. Por ejemplo, hay algunos protocolos que están asociados a la navegación de redes ([21]), otros son para la transferencia de ficheros ([22]), etc. Por tanto, las técnicas de inspección basadas en la inspección de protocolos y combinadas con el análisis estadístico tienen como fin buscar determinadas pautas o impresiones dactilares que determinan los protocolos que están presentes ([23]). Estas técnicas de inspección permiten a los PSI entender el tipo de comunicación (correo electrónico, navegación de redes, subida de archivos) y, en algunos casos, identificar el servicio específico o la aplicación utilizada, como es el caso de algunas comunicaciones VoIP en que los protocolos utilizados son muy específicos hacia un vendedor concreto o proveedor de servicios. El propio conocimiento del tipo de comunicación permite a los PSI aplicar determinadas políticas de gestión del tráfico, por ejemplo, para bloquear el tráfico de la red. También puede ser el primer paso para permitir al PSI realizar otros análisis que puedan requerir un acceso completo a los metadatos y al contenido de la comunicación.

([20]) Sin embargo, el equipo de red de internet utiliza protocolos de encaminamiento que registran la actividad, procesan estadísticas del tráfico e intercambian información con otros equipos de red, a fin de encaminar los paquetes IP utilizando la vía más eficiente. Por ejemplo, cuando un enlace está congestionado o roto y el encaminador recibe esta información, actualizará su tabla de encaminamiento con alguna alternativa que no utilice dicho enlace. Cabe asimismo señalar que la obtención y el tratamiento en algunos casos podrá hacerse con fines de facturación o incluso de conformidad con los requisitos de la Directiva de conservación de datos.

([21]) HTTP — Hypertext transfer protocol (Protocolo de transferencia de hipertexto) — o HTML — Hypertext Markup Language (Lenguaje de marcado de hipertexto).

([22]) FTP — File transfer protocol (Protocolo de transferencia de archivos).

([23]) Existen distintos modos de identificar los protocolos utilizados. Por ejemplo, es posible buscar en campos específicos de los protocolos internos, por ejemplo, para identificar los puertos utilizados para establecer la comunicación. También puede deducirse del análisis de algunos campos específicos, una caracterización estadística del flujo de la comunicación, así como la correlación de los protocolos utilizados simultáneamente entre dos direcciones IP.

— *Inspección profunda de paquetes basada en el análisis del contenido de la comunicación*. Por último, también es posible inspeccionar los metadatos ([24]) y el contenido de la propia comunicación. Esta técnica consiste en la intercepción de todos los paquetes IP que forman parte del flujo de comunicación original de modo que el contenido original de la comunicación puede ser totalmente reconstruido y analizado. Por ejemplo, para detectar contenido perjudicial o ilegal como virus, pornografía infantil, etc., es necesario reconstruir el propio contenido para que pueda ser analizado. Cabe señalar que algunas veces la comunicación puede estar explícitamente encriptada de extremo a extremo por las partes implicadas y esta práctica impedirá a los PSI realizar el análisis del contenido de la comunicación.

### IV.3. **Implicaciones relativas a la protección de datos y a la intimidad**

33. Las técnicas de inspección basadas en las cabeceras de IP y, más concretamente, aquellas basadas en la inspección de paquetes implican la supervisión y el filtrado de estos datos y tienen graves implicaciones desde el punto de vista de la protección de datos y la intimidad. Asimismo, también pueden entrar en conflicto con el derecho de confidencialidad de las comunicaciones.

34. Mirar las comunicaciones de las personas ya tiene de por sí graves implicaciones para la protección de datos y la intimidad. Sin embargo, el problema es más amplio ya que, en función de los efectos perseguidos con la supervisión y la intercepción, pueden verse aumentadas las implicaciones para la intimidad. De hecho, no es lo mismo inspeccionar simplemente las comunicaciones, por ejemplo, para garantizar que el sistema funciona bien que inspeccionar las comunicaciones para aplicar políticas que pueden tener un impacto sobre las personas. Cuando el tráfico y las políticas de selección sólo busquen evitar la congestión de la red, normalmente no tendrán mayores implicaciones sobre la intimidad de las personas. Sin embargo, las políticas de gestión del tráfico pueden buscar bloquear alguna información del contenido o influir en la comunicación, por ejemplo, a través de la publicidad comportamental. En dichos casos, los efectos son más intrusivos. La preocupación se torna más crítica si nos damos cuenta de que este tipo de información podría ser obtenido no para un pequeño grupo de personas sino más bien sobre una base generalizada, para todos los clientes del PSI ([25]). Si todos los PSI adoptan técnicas de filtrado, esto puede conducir a una supervisión generalizada del uso de internet. Además, si nos centramos en el tipo de información que está siendo tratada, los riesgos para la intimidad obviamente son altos, así como la información que se obtiene es posible que sea muy sensible y que, tras su obtención, esté disponible para los PSI y para aquellos que busquen información de los mismos. Además, la información también podría resultar muy valiosa desde el punto de vista comercial, lo cual representa en sí mismo un alto riesgo de deriva funcional en la que los fines iniciales fácilmente podrían evolucionar hacia una explotación comercial o de otro tipo de la información obtenida.

35. La correcta aplicación de las técnicas de supervisión, inspección y filtrado debe llevarse a cabo de conformidad con las garantías de protección de datos y de intimidad que resulten aplicables, las cuales establecen límites sobre qué cosas pueden hacerse y en qué circunstancias. A continuación se recoge un panorama general de las garantías aplicables del actual marco jurídico de la protección de datos y la intimidad de la Unión Europea.

## V. **APLICACIÓN DEL MARCO JURÍDICO DE LA PROTECCIÓN DE DATOS Y LA INTIMIDAD DE LA UNIÓN EUROPEA**

36. El marco jurídico de la protección de datos de la Unión Europea es tecnológicamente neutro y como tal no regula las técnicas de inspección específicas descritas anteriormente. La Directiva sobre la privacidad y las comunicaciones electrónicas regula la privacidad en el suministro de servicios de comunicación

([24]) Cada protocolo posee algunos campos específicos en su cabecera que ofrecen información informal adicional sobre la comunicación que está siendo transmitida. Por lo tanto, puede decirse que el contenido de dichos campos son los metadatos de la comunicación. Un ejemplo de estos campos puede ser el número de puerto utilizado, cuando, por ejemplo, si el número es 80, es muy probable que el tipo de comunicación sea navegación de redes.

([25]) Por supuesto, las capacidades de seguimiento no son exclusivas de los PSI. Los proveedores de publicidad en la red, por ejemplo, también pueden, a través del uso de *cookies* de terceros, seguir a los usuarios a través de los sitios web. Véase a modo de ejemplo, un artículo académico reciente que demuestra que Google tiene presencia en 97 de los 100 sitios web principales, lo que significa que Google puede seguir a los usuarios que hayan bloqueado las *cookies* de terceros cuando naveguen por estos populares sitios web. Véase: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (29 de julio de 2011). Disponible en SSRN: http://ssrn.com/abstract=1898390. El seguimiento de usuarios a través de las *cookies* de terceros ha sido tratado por el Grupo de Trabajo del Artículo 29. Véase el Dictamen 2/2010 sobre publicidad comportamental en línea, adoptado el 22 de junio de 2010 (WP 171).

electrónica en redes públicas (de manera típica, el acceso a internet y la telefonía) ([26]) y la Directiva sobre protección de datos regula el tratamiento de datos en general. Considerado en su conjunto este marco jurídico establece distintas obligaciones que se aplican a los PSI que tratan y supervisan el tráfico y los datos de las comunicaciones.

### V.1. **Fundamentos jurídicos para tratar los datos de tráfico y los datos sobre contenidos**

37. En virtud de la legislación de protección de datos, el tratamiento de datos personales, como en este caso, el tratamiento los datos de tráfico y de las comunicaciones, exige una base jurídica adecuada. Además de este requisito general, pueden aplicarse requisitos específicos en determinados casos.

38. En este caso, el tipo de datos personales que los PSI tratan se refieren a los datos de tráfico y al contenido de las comunicaciones. El contenido de las comunicaciones y los datos de tráfico están protegidos por el derecho de confidencialidad de la correspondencia, garantizado por el artículo 8 del CEDH y los artículos 7 y 8 de la Carta. Más concretamente, el artículo 5, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas, titulado «confidencialidad de las comunicaciones», exige que los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. Al mismo tiempo, el artículo 5, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas prevé que se permitirá el tratamiento de los datos de tráfico y del contenido por parte de los PSI, en determinadas circunstancias, con el consentimiento de los usuarios. Esto se hace estableciendo la prohibición de «la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15.». Esto se desarrolla con más detalle a continuación.

39. Además del consentimiento de los usuarios interesados, la Directiva sobre la privacidad y las comunicaciones electrónicas prevé otros fundamentos que pueden legitimar el tratamiento de los datos de tráfico y de las comunicaciones por parte de los PSI. Los fundamentos jurídicos pertinentes para el tratamiento en este caso son (i) ofrecer el servicio; (ii) garantizar la seguridad del servicio, y (iii) minimizar la congestión. Otros posibles motivos que pueden legitimar las políticas de gestión basadas en los datos de tráfico y de las comunicaciones serán tratados en el inciso (iv).

#### i) Fundamentos jurídicos para ofrecer el servicio

40. Tal como se ha ilustrado en el apartado IV, los PSI tratan la información sobre las cabeceras de IP para fines que consisten en encaminar cada paquete de IP hacia su destino. El artículo 6, apartados 1 y 2, de la Directiva sobre la privacidad y las comunicaciones electrónicas permite el tratamiento de datos de tráfico a efectos de la conducción de una comunicación. Por lo tanto, los PSI pueden tratar la información que sea necesaria para ofrecer el servicio.

#### ii) Fundamentos jurídicos para garantizar la seguridad del servicio

41. De conformidad con lo dispuesto en el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas, los PSI tiene la obligación general de adoptar las medidas adecuadas para preservar la seguridad de sus servicios. La práctica de filtrar virus puede implicar el tratamiento de cabeceras de IP y de carga útil de IP. Teniendo en cuenta que el artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas exige a los PSI que garanticen la seguridad de la red, esta disposición legitima las técnicas de inspección basadas en las cabeceras de IP y el contenido que tienen estrictamente como fin conseguir dicho objetivo. En la práctica, esto significa que, dentro de los límites establecidos por el principio de proporcionalidad (véase el apartado V.3), los PSI pueden realizar la supervisión y el filtrado de los datos de las comunicaciones para luchar contra los virus y garantizar de manera general la seguridad de la red ([27]).

([26]) El artículo 1, apartado 10, de la Directiva sobre la privacidad y las comunicaciones electrónicas tiene la siguiente redacción: «En el sector de las comunicaciones electrónicas es de aplicación la Directiva 95/46/CE, en particular para todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no están cubiertas de forma específica por las disposiciones de la presente Directiva, incluidas las obligaciones del responsable del tratamiento de los datos y los derechos de las personas». Asimismo, el considerando 17 resulta pertinente en cuanto al consentimiento del interesado: «A efectos de la presente Directiva, el consentimiento de un usuario o abonado, independientemente de que se trate de una persona física o jurídica, debe tener el mismo significado que el consentimiento de la persona afectada por los datos tal como se define y se especifica en la Directiva 95/46/CE.».

([27]) Dictamen 2/2006 del Grupo de Trabajo del Artículo 29 sobre el respeto de la privacidad en relación con la prestación de servicios de cribado de correo electrónico, adoptado el 21 de febrero de 2006 (WP 118). En este dictamen el Grupo de Trabajo considera que la utilización de filtros con los fines establecidos en el artículo 4 puede ser compatible con el artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas.

iii) Fundamentos jurídicos para minimizar los efectos de la congestión

42. La lógica de este fundamento jurídico se encuentra en el considerando 22 de la Directiva sobre la privacidad y las comunicaciones electrónicas, que explica la prohibición de almacenar comunicaciones del artículo 5, apartado 1. Lo anterior no prohíbe los almacenamientos automáticos, intermedios y transitorios en la medida en que tengan lugar con el único objeto de realizar la transmisión y no duren más de lo necesario a efectos de la transmisión y de la gestión del tráfico, y se siga garantizando la confidencialidad de las comunicaciones.

43. Si existe congestión, se plantea la cuestión de si los PSI pueden considerar hacer caer o retrasar el tráfico de manera aleatoria o bien ralentizar las comunicaciones para las que el factor del tiempo no es importante, por ejemplo, las comunicaciones P2P o el tráfico de correos electrónicos, permitiendo, por ejemplo, que el tráfico de voz circule con una calidad aceptable.

44. Dado el interés general de la sociedad de garantizar una red de comunicaciones utilizable, los PSI podrían argumentar que dar prioridad o regular el tráfico para solucionar la congestión es una medida legítima que resulta necesaria para ofrecer un servicio apropiado, lo cual significa que en estos casos y a estos efectos, existiría un fundamento jurídico general para tratar los datos personales y que no sería necesario un consentimiento específico por parte de los usuarios.

45. Al mismo tiempo, la capacidad de interferir de este modo no es ilimitada. Si los PSI precisan inspeccionar las comunicaciones desde la perspectiva de la confidencialidad y aplicar de manera estricta el principio de proporcionalidad, deberán utilizar al menos un método disponible menos intrusivo para lograr dicho propósito (evitando una inspección profunda de paquetes), que deberán aplicar mientras sea necesario para resolver la congestión.

iv) Fundamentos jurídicos para tratar datos para otros fines

46. Los PSI también pueden desear inspeccionar los datos de tráfico y los datos de los contenidos con otros fines, por ejemplo, ofrecer abonos especiales (por ejemplo, un abono que limite el acceso a las comunicaciones P2P o un abono que aumente la velocidad para determinadas aplicaciones). La inspección y posterior uso de los datos de tráfico y de las comunicaciones para fines distintos de ofrecer el servicio o garantizar la seguridad del mismo y la falta de congestión únicamente queda permitido en condiciones estrictas, de conformidad con lo dispuesto en el marco jurídico.

47. El marco jurídico es principalmente el artículo 5, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas que exige el consentimiento por parte de los usuarios interesados para escuchar, grabar, almacenar u otro tipo de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados. En la práctica esto significa que el consentimiento de los usuarios implicados en una comunicación es necesario para legitimar el tratamiento tanto de los datos de tráfico como de las comunicaciones, en virtud de lo dispuesto en el artículo 5, apartado 1.

48. Tal como se ha explicado anteriormente, la aplicación de las técnicas de inspección y filtrado se basa tanto en las cabeceras de IP, que constituyen los datos de tráfico, como en la inspección profunda de paquetes que también implican a las cargas útiles de IP y constituyen datos de comunicación. Por lo tanto, en principio, la aplicación de dichas técnicas para efectos distintos de la conducción del servicio o la seguridad estarían prohibidos, salvo si existe un fundamento legítimo que permita el tratamiento, como el consentimiento (artículo 5, apartado 1). Un ejemplo en el que resultaría aplicable el artículo 5, apartado 1, es cuando un PSI decide ofrecer a los clientes una tarifa reducida de acceso a internet a cambio de recibir publicidad comportamental, utilizando de este modo para ello la inspección profunda de paquetes. Un consentimiento real, específico e informado resulta necesario, según lo dispuesto en el artículo 5, apartado 1.

49. Además, el artículo 6 de la Directiva sobre la privacidad y las comunicaciones electrónicas titulado «Datos de tráfico» establece ciertas normas que se aplican específicamente a los datos de tráfico. Más

concretamente, prevé la posibilidad de que los PSI traten datos de tráfico basados en el consentimiento de los usuarios para recibir servicios con valor añadido ([28]). Esta disposición especifica el requisito del consentimiento previsto en el artículo 5, apartado 1, cuando hay datos de tráfico en juego.

50. En la práctica, no siempre puede ser fácil determinar, por ejemplo, en qué casos el consentimiento es necesario y en qué casos la seguridad de la red puede legitimar el tratamiento, en especial si el objetivo de las técnicas de inspección es doble (por ejemplo, evitar la congestión y ofrecer servicios con valor añadido). Debe hacerse hincapié en que el consentimiento no puede ser considerado una salida fácil y sistemática para cumplir los principios de la protección de datos.

51. La experiencia no es mucha en cuanto a la aplicación del marco y, más concretamente, sobre los diversos aspectos que se han destacado anteriormente. Éste es un ámbito en que resulta esencial una mayor orientación, tal como se ha desarrollado en el apartado IV. Además, existen otros aspectos relevantes relacionados con la obtención del consentimiento que también merecen una especial consideración. Estos se describen a continuación.

### V.2. **Cuestiones relativas al consentimiento expreso informado como fundamento jurídico**

52. El consentimiento que exigen los artículos 5 y 6 de la Directiva sobre la privacidad y las comunicaciones electrónicas tiene el mismo significado que el consentimiento del interesado tal como se define y especifica en la Directiva 95/46/CE ([29]). Según el artículo 2, letra h), de la Directiva sobre protección de datos, «el consentimiento del interesado» es «toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan.». Recientemente, el papel del consentimiento y los requisitos para que el mismo sea válido han sido tratados por el Grupo de Trabajo del Artículo 29 en su Dictamen 15/2011 sobre la definición del consentimiento ([30]).

53. Los PSI que soliciten el consentimiento para realizar la inspección y el filtrado de los datos de tráfico y de los contenidos deberán garantizar, por tanto, que el consentimiento es libre y específico, y deberá existir una manifestación de voluntad totalmente informada de la persona mediante la cual establezca su acuerdo a que se traten datos personales que le conciernan. El considerando 17 de la Directiva sobre la privacidad y las comunicaciones electrónicas reitera esto «(…) el consentimiento podrá darse por cualquier medio apropiado que permita la manifestación libre, inequívoca y fundada de la voluntad del usuario, por ejemplo mediante la selección de una casilla de un sitio web en internet». A continuación se ofrecen algunos ejemplos prácticos de lo que significa en este contexto un consentimiento libre, específico e informado.

*Consentimiento: manifestación de voluntad libre, específica e informada*

54. *Consentimiento libre*. Los usuarios no deben padecer limitaciones vinculadas al consentimiento para el abono de internet que desean contratar.

55. El consentimiento de las personas no habrá sido libremente dado si deben consentir la supervisión de sus datos de comunicación para obtener acceso al servicio de comunicación. Esto sería aún más cierto si todos los proveedores de un determinado mercado se implican en la gestión del tráfico con fines que van más allá de la seguridad de la red. La única opción que resta no sería en absoluto suscribirse a un

([28]) El considerando 18 de la Directiva incluye una lista con ejemplos de servicios con valor añadido. No queda claro si puede interpretarse que los servicios para los que se aplican las políticas de gestión del tráfico formen parte de la lista. Puede entenderse que las políticas de gestión del tráfico destinadas a dar prioridad a determinado contenido ofrecen calidad al servicio. Por ejemplo, la gestión del tráfico que implique simplemente el tratamiento de cabeceras de IP y que tenga como fin ofrecer servicios de juego con precios especiales, en que se dé prioridad al tráfico del juego personal de los usuarios a través de la red podría considerarse un servicio con valor añadido. Por otro lado, está lejos de quedar claro si la gestión del tráfico suprime determinados tipos de tráfico, por ejemplo, bajar de categorías al tráfico de igual a igual podría ser considerado como un modo de suprimirlo.

([29]) Véanse el considerando 17 y el artículo 2, letra f), de la Directiva sobre la privacidad y las comunicaciones electrónicas.

([30]) Adoptado el 13 de julio de 2011 (WP 187).

servicio de internet. Dado que internet se ha convertido en una herramienta fundamental a efectos tanto de trabajo como de ocio, no abonarse a un servicio de internet no es una alternativa válida. El resultado sería que los individuos podrían no tener una opción real, es decir, que no podrían dar su consentimiento libremente ([31]).

56. El SEPD considera que existe una necesidad clara de que la Comisión y las autoridades nacionales controlen el mercado, en especial para determinar si este panorama, es decir, que los proveedores vinculen los servicios de telecomunicaciones a la supervisión de las comunicaciones, se convierte en una tendencia general. Los proveedores deberían ofrecer servicios alternativos, incluido un abono a internet que no estuviese sometido a la gestión del tráfico, sin imponer mayores costes a las personas.

57. *Consentimiento específico*. La necesidad de que el consentimiento sea específico exige en este caso que los PSI procuren el consentimiento para supervisar los datos de tráfico y de las comunicaciones de un modo claro y distintivo. Según el Grupo de Trabajo del Artículo 29, «… para ser específico, el consentimiento debe ser comprensible: referirse de manera clara y precisa al alcance y las consecuencias del tratamiento de datos. No puede referirse a un conjunto indefinido de actividades de tratamiento. Esto significa, en otras palabras, que el consentimiento se aplica en un contexto limitado.». No es posible obtener un consentimiento específico si el consentimiento para la inspección de los datos de tráfico y de las comunicaciones está «ligado» a un consentimiento general de contratar el servicio. En su lugar, el carácter específico exige el uso de medios especiales para obtener el consentimiento, como un formulario de consentimiento específico o una casilla separada claramente dedicada a efectos de la supervisión (en lugar de introducir la información en las condiciones generales del contrato y exigir la firma del contrato tal como está).

58. *Consentimiento informado*. Para ser válido, el consentimiento tiene que ser informado. La necesidad de proporcionar una información previa adecuada deriva no solo de la Directiva sobre la privacidad y las comunicaciones electrónicos y la Directiva sobre protección de datos sino también de los artículos 20 y 21 de la Directiva de servicio universal, modificada por la Directiva 2009/136/CE ([32]). La necesidad de información y de consentimiento está expresamente confirmada en el considerando 28 de la Directiva 2009/136/CE: «debe facilitarse en cualquier caso a los usuarios información completa sobre cualquier limitación que imponga el proveedor del servicio o de la red en la utilización de los servicios de comunicaciones electrónicas. Dicha información debe especificar, a elección del proveedor, bien sea el tipo de contenido, la aplicación o el servicio de que se trate, bien las aplicaciones o los servicios individuales, bien ambas cosas.». A continuación especifica que: «en función de la tecnología que se utilice y del tipo de limitación, dichas limitaciones pueden requerir el consentimiento del usuario en virtud de la Directiva 2002/58/CE.».

59. Dada la complejidad de estas técnicas de supervisión, facilitar una información previa significativa es uno de los principales retos para obtener un consentimiento válido. Debería informarse a los consumidores de un modo en que pudieran entender la información que está siendo tratada, el modo en que se está utilizando y el impacto sobre la experiencia del usuario y el nivel de intromisión en la intimidad relacionado con estas técnicas.

60. Esto implica no solo que la propia información debe ser clara y comprensible para los usuarios medios sino también que la información se facilita directamente a las personas de un modo visible de modo que no puedan obviarla.

61. *Manifestación de voluntad*. El consentimiento según el marco jurídico aplicable también requiere una acción positiva por parte del usuario que manifieste su acuerdo. El consentimiento implícito no cumple este estándar. Esto también confirma la necesidad de utilizar medios especiales para obtener el consentimiento que permita a los PSI inspeccionar los datos de tráfico y de comunicaciones en el contexto de la aplicación de las políticas de gestión del tráfico. En su reciente dictamen relativo a la definición del consentimiento, el Grupo de Trabajo del Artículo 29 destacó la necesidad de precisión a la hora de obtener el consentimiento con respecto a los diferentes elementos del tratamiento de datos.

([31]) Un caso similar ocurre con los datos PNR cuando se discutió si era válido el consentimiento de los pasajeros para transmitir la información de la reserva a las autoridades de los Estados Unidos. El Grupo de Trabajo consideró que el consentimiento de los pasajeros no se da libremente ya que las compañías aéreas están obligadas a enviar los datos antes de la salida del vuelo y que los pasajeros no tienen, por tanto, una opción real si desean volar; Dictamen 6/2002 del Grupo de Trabajo del Artículo 29 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos.

([32]) Directiva 2009/136/CE de 25 de noviembre de 2009 por la que se modifica la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (véase la nota a pie de página nº 15).

62. Se podría argumentar que si las partes implicadas en una comunicación no desean que los PSI la intercepten para aplicar las políticas de gestión del tráfico, siempre pueden encriptar la comunicación. Este enfoque puede considerarse útil desde el punto de vista práctico, aunque requiere algún esfuerzo y conocimientos técnicos y no puede ser considerado similar a un consentimiento libre, específico e informado. Asimismo, la utilización de las técnicas de encriptado no hace que la comunicación sea totalmente confidencial ya que el PSI puede acceder al menos a la información de la cabecera de IP para encaminar la comunicación y también estaría en posición de aplicar un análisis estadístico.

63. Según lo dispuesto en el artículo 5, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas, el consentimiento debe ser obtenido de los usuarios interesados. En muchos casos, el usuario será la misma persona que el abonado, lo cual permite obtener el consentimiento en el momento del abono a un servicio de telecomunicaciones. En otros casos, incluidos aquellos en que estén implicadas más de una persona, será necesario obtener por separado el consentimiento de los usuarios interesados, lo cual puede plantear los problemas prácticos que se indican a continuación.

*Consentimiento de todos los usuarios interesados*

64. El artículo 5, apartado 1, establece que el consentimiento del usuario legitima el tratamiento. El consentimiento debe ser obtenido de *todos los usuarios* implicados en la comunicación. La lógica detrás de esto es que la comunicación normalmente afecta, como mínimo, a dos personas (el remitente y el destinatario). Por ejemplo, si un PSI escanea las cargas útiles de IP que se refieren a un correo electrónico, existe información de inspección que guarda relación tanto con el remitente como con el destinatario del mensaje.

65. Al supervisar e interceptar el tráfico y las comunicaciones (por ejemplo, algún tráfico de la red), puede que a los PSI les baste obtener el consentimiento del usuario, es decir, del abonado. Esto es porque la otra parte de la comunicación, en este caso, el sitio web visitado, puede no ser considerado un «usuario interesado» ([33]). Sin embargo, la situación puede ser más compleja cuando dicha supervisión implica la inspección del contenido de los correos electrónicos y, por tanto, la información personal del remitente y del destinatario del mensaje, quienes pueden no tener una relación contractual con el mismo PSI. De hecho, en estos casos, el PSI estaría tratando datos personales (nombre, dirección de correo electrónico y datos de contenido potencialmente sensible) de personas que no son clientes. Desde un punto de vista práctico, la obtención del consentimiento de dichas personas puede ser más difícil ya que debería hacerse caso por caso, en lugar de en el momento de contratación del servicio de telecomunicaciones. Tampoco sería realista asumir que el consentimiento del abonado fue proporcionado en nombre de otros usuarios, como suele ser el caso en los hogares particulares.

66. En dicho contexto, el SEPD considera que los PSI deberían respetar los requisitos legales existentes e implantar políticas que no impliquen la supervisión y la inspección de información. Esto es todavía más importante respecto de los servicios de comunicación que implican a terceros que no pueden dar su consentimiento a la supervisión, en especial por lo que se refiere a los mensajes enviados y recibidos (esto no es aplicable cuando el fin está basado en consideraciones de seguridad).

67. Al mismo tiempo, debe señalarse que la legislación nacional de aplicación del artículo 5, apartado 1, de la Directiva sobre la privacidad y las comunicaciones electrónicas no siempre puede resultar satisfactoria en relación con este punto y que, en general, parece existir más bien una necesidad de una mayor orientación en relación con los requisitos de dicha Directiva en este contexto. El SEPD invita, por tanto, a la Comisión a asumir un papel más activo en este sentido y adoptar una iniciativa que se beneficie de las aportaciones de las autoridades de supervisión recogidas en el Grupo de Trabajo del Artículo 29 y de otras partes implicadas. Si fuera necesario, deberá presentarse un asunto ante el Tribunal de Justicia con el fin de proporcionar una total claridad respecto del significado y de las consecuencias del artículo 5, apartado 1.

([33]) Sin perjuicio de los casos en que el tráfico de la red implique la transmisión de información personal como, por ejemplo, fotografías de personas físicas identificables colgadas en un sitio web. El tratamiento de dicha información exige una base jurídica aunque no estará cubierto por el artículo 5, apartado 1, ya que dichas personas no se considerarán «usuarios interesados».

### V.3. **Proporcionalidad — principio de minimización de los datos**

68. El artículo 6, letra c), de la Directiva sobre protección de datos establece el principio de proporcionalidad ([34]), que es aplicable tanto a los PSI como a los responsables del tratamiento de datos en el sentido de lo dispuesto en dicha Directiva, cuando participan en la supervisión y el filtrado.

69. En virtud de dicho principio, los datos personales podrán tratarse únicamente en la medida en que sean «adecuados, pertinentes y no excesivos en relación con el fin para el que se obtienen o tratan». La aplicación de este principio implica la necesidad de elaborar una evaluación sobre si los medios empleados para el tratamiento de datos y los tipos de datos personales utilizados son adecuados y si pueden ser razonablemente utilizados para alcanzar sus objetivos. Si la conclusión es que se obtienen más datos de lo que es necesario, entonces no se cumple este principio.

70. La conformidad con el principio de proporcionalidad de determinados tipos de técnicas de inspección deberá valorarse caso por caso, ya que no es posible extraer conclusiones en abstracto. Sin embargo, es posible indicar diversos aspectos concretos que deberían ser evaluados al valorar el cumplimiento del principio de proporcionalidad.

71. *La cantidad de información tratada*. La vigilancia de las comunicaciones de los clientes de los PSI en sus niveles más altos posibles será, en la mayoría de los casos, excesiva e ilegal. El hecho de que esto pueda llevarse a cabo a través de medios que no son aparentes para las personas y de que sea difícil que las mismas entiendan qué es lo que está ocurriendo aumenta el impacto sobre su intimidad. Los PSI deberían valorar qué medios menos intrusivos pueden estar disponibles para lograr el resultado que se pretende. Por ejemplo, ¿puede la supervisión de las cabeceras de IP lograr el resultado deseado en lugar de tener que realizar una inspección profunda de paquetes? Incluso cuando se utiliza la inspección profunda de paquetes, la identificación de sólo ciertos protocolos puede proporcionar la información necesaria. La aplicación de las garantías de protección de datos, incluido el hecho de hacer que los datos sean pseudoanónimos, puede también ser relevante. La conclusión de la evaluación debe confirmar que el tratamiento de datos es proporcional.

72. *Los efectos del tratamiento (directamente vinculados a los fines)*. Puede faltar proporcionalidad en los casos en que los PSI utilizan las políticas de gestión del tráfico excluyendo el acceso a determinados servicios, sin permitir que los usuarios disfruten, a cambio, de una participación equitativa del beneficio resultante.

73. Es importante recordar que el principio de proporcionalidad continúa siendo de aplicación incluso si se han satisfecho otros requisitos legales obligatorios, incluso si un PSI ha obtenido, por ejemplo, el consentimiento de las personas para llevar a cabo una supervisión del contenido. Esto quiere decir que el tratamiento de datos llevado a cabo a través de la supervisión del contenido aún podría ser ilegal si vulnera el principio fundamental de proporcionalidad subyacente.

### V.4. **Medidas organizativas y de seguridad**

74. El artículo 4 de la Directiva sobre la privacidad y las comunicaciones electrónicas exige explícitamente a los PSI que adopten medidas técnicas y de gestión para garantizar que (i) solo el personal autorizado tenga acceso a los datos personales para autorizados por la ley; (ii) se protegen los datos personales de los tratamientos accidentales o ilícitos, y (iii) se aplica una política de seguridad con respecto al tratamiento de datos personales. También permite a las autoridades nacionales competentes examinar estas medidas.

75. Asimismo, según lo dispuesto en el artículo 4, apartados 2 y 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas, los PSI también notificarán adecuadamente tanto las autoridades nacionales competentes en caso de violación de los datos, como a los particulares en el supuesto de que la difusión pueda afectarles negativamente.

76. El tratamiento de la información personal incluida en las comunicaciones con el objetivo de aplicar políticas de gestión del tráfico puede dar acceso a los PSI a datos que sean incluso más sensibles que los datos de tráfico.

([34]) Tal como se ha destacado anteriormente, la Directiva sobre protección de datos es aplicable a todas las cuestiones relativas a la protección de los derechos y las libertades fundamentales que no estén cubiertas de forma específica por las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas.

77. Por lo tanto, las políticas de seguridad desarrolladas por los PSI deberían incorporar salvaguardias específicas que garanticen que las medidas adoptadas son adecuadas para estos riesgos. Al mismo tiempo, las autoridades nacionales competentes que examinen dichas medidas deben ser especialmente exigentes. Por último, debería garantizarse que se establecen procedimientos de notificación efectivos para informar a los interesados sobre la información que se ha visto comprometida y quienes pueden resultar afectados negativamente.

## VI. **SUGERENCIAS PARA LAS MEDIDAS POLÍTICAS Y LEGISLATIVAS**

78. Las técnicas de inspección basadas en los datos de tráfico y en la inspección de las cargas útiles de IP, es decir, el contenido de la comunicación, pueden revelar la actividad en internet de los usuarios, como los sitios web visitados y las actividades en dichos sitios, el uso de aplicaciones P2P, los ficheros descargados, los mensajes enviados y recibidos, los remitentes, los asuntos y los términos de los mismos, etc. Los PSI pueden desear utilizar esta información para dar prioridad a algunas comunicaciones respecto de otras, como los vídeos a la carta. Pueden desear utilizarla para identificar virus o elaborar perfiles que sirvan a efectos de la publicidad comportamental. Estas acciones interfieren en el derecho de confidencialidad de las comunicaciones.

79. En función de las técnicas utilizadas y de las especificaciones del asunto, las implicaciones sobre la intimidad pueden verse aumentadas. Cuando más profunda sea la intercepción y el análisis de la información obtenida, mayor será el conflicto con el principio de confidencialidad de las comunicaciones. Los fines para los que la supervisión tiene lugar y las garantías de protección de datos que se hayan aplicado también son elementos fundamentales para determinar el grado de intrusión en los datos personales y la intimidad de los particulares. El bloqueo y la supervisión con fines de combatir el código malicioso (*malware*), con limitaciones estrictas sobre la conservación y el uso de los datos inspeccionados no pueden compararse con las situaciones en que la información queda registrada para elaborar perfiles individuales a efectos de la publicidad comportamental.

80. En principio, el SEPD considera que el marco existente de la protección de datos y la intimidad de la Unión Europea si se interpreta, aplica y refuerza adecuadamente sería adecuado para garantizar que se cumple el derecho a la confidencialidad y, en general, que la protección de la protección de datos y la intimidad de los particulares no se ve menoscabada ([35]). Los PSI no deberían utilizar dichos mecanismos salvo si el marco jurídico ha sido aplicado adecuadamente. Más concretamente, entre los elementos fundamentales del marco que los PSI deberían considerar y respetar se incluyen los siguientes:

— los PSI pueden aplicar políticas de gestión del tráfico destinadas a proporcionar seguridad en el servicio, al ofrecer el servicio, incluida la limitación de la congestión, según lo dispuesto en los artículos 4 y 6 de la Directiva sobre la privacidad y las comunicaciones electrónicas,

— los PSI precisan otro fundamento jurídico específico, y posiblemente el consentimiento de los usuarios, para aplicar las políticas de gestión del tráfico que impliquen el tratamiento de los datos de tráfico o datos de la comunicación con fines distintos de los mencionados anteriormente. Por ejemplo, el consentimiento informado de los usuarios es necesario para supervisar y filtrar las comunicaciones de los particulares a efectos de limitar (o permitir) el acceso a determinadas aplicaciones y servicios como los P2P o VoIP,

— el consentimiento debe ser libre, explícito e informado y debe ser manifestado a través de una acción positiva. Estos requisitos ponen un fuerte énfasis en la necesidad de intensificar los esfuerzos para garantizar que los particulares están adecuadamente informados, de un modo directo, comprensible y específico, de modo que puedan valorar los efectos de las prácticas y, en última instancia, adoptar una decisión informada. Dada la complejidad de estas técnicas de supervisión, facilitar una información previa significativa a los usuarios es uno de los principales retos para obtener un consentimiento válido. Además, no deberían existir consecuencias perjudiciales (incluidos los costes económicos) para los usuarios que no dan su consentimiento para dicha supervisión,

([35]) Esto se entiende sin perjuicio de la necesidad de modificar la ley sobre la base de otras consideraciones, en especial en el contexto de una revisión general del marco jurídico de la Unión Europea para la protección de datos, con vistas a hacerlo más eficaz como consecuencia de las nuevas tecnologías y la globalización.

— el principio de proporcionalidad juega un papel crucial cuando los PSI establecen políticas de gestión del tráfico, con independencia de la base jurídica para el tratamiento y su finalidad: suministrar el servicio, evitar la congestión u ofrecer abonos especiales con o sin acceso a determinados servicios y aplicaciones. Este principio limita la capacidad de los PSI de realizar una supervisión del contenido de las comunicaciones de los particulares que pueda implicar el tratamiento de información excesiva o únicamente aumentar los beneficios de dichos proveedores. Lo que el PSI puede llevar a cabo desde un punto de vista logístico dependerá del nivel de intrusión de las técnicas, los resultados pretendidos (para lo cual pueden aumentar los beneficios) y las garantías de protección de datos y la intimidad específicas aplicadas. Antes de implantar las técnicas de inspección, los PSI deben llevar a cabo una valoración de si dichas técnicas cumplen el principio de proporcionalidad.

81. Aunque actualmente el marco jurídico incluye las condiciones y garantías pertinentes, existe la necesidad de prestar una especial atención al hecho de si los PSI cumplen de manera eficaz los requisitos legales, de si proporcionan la información necesaria para que los consumidores hagan elecciones con sentido y de si observan el principio de proporcionalidad. A escala nacional, entre las autoridades competentes para realizar lo anterior, están incluidas las autoridades nacionales de telecomunicaciones, por un lado, y por otro, las autoridades nacionales encargadas de la protección de datos. A escala europea, entre los organismos relevantes se incluye el ORECE. El SEPD también podrá jugar un papel en este contexto.

82. Además de supervisar el presente nivel de cumplimiento, dada lo relativamente nuevo de la posibilidad de llevar a cabo la inspección masiva y en tiempo real de comunicaciones, en el presente dictamen se han debatido algunos aspectos relacionados con la aplicación del marco que requieren un análisis más profundo y una mayor aclaración. Una orientación especialmente pertinente en diversos ámbitos incluye:

— determinar las prácticas de inspección que son legítimas para garantizar la fluidez del tráfico, lo cual puede no exigir el consentimiento por parte de los usuarios como, por ejemplo, la lucha contra el correo no deseado. Además del carácter intrusivo de la supervisión aplicada, son importantes aspectos como, por ejemplo, el nivel de perturbación de la fluidez del tráfico que podría ocurrir de otro modo,

— determinar qué técnicas de inspección pueden llevarse a cabo con fines de seguridad, que no precisarán el consentimiento por parte de los usuarios,

— determinar cuándo la supervisión exige el consentimiento por parte de los particulares, en especial el consentimiento de todos los usuarios interesados, así como los parámetros técnicos permitidos para garantizar que la técnica de inspección no implica un tratamiento de datos desproporcionado para los efectos que se pretenden,

— además de los tres casos anteriores, puede ser necesaria una orientación relativa a la aplicación de las garantías necesarias de protección de datos (limitación a una finalidad específica, seguridad, etc.).

83. Dado que las competencias en este ámbito son tanto nacionales como europeas, el SEPD considera que es esencial compartir opiniones y experiencias para hallar enfoques armonizados. Para ello, el SEPD sugiere la creación de una plataforma o grupo de expertos que pueda reunir a los representantes de las autoridades nacionales de reglamentación, al Grupo de Trabajo del Artículo 29, al SEPD y al ORECE. El primer objetivo de dicha plataforma sería desarrollar orientaciones, al menos sobre los elementos identificados anteriormente, para garantizar enfoques sólidos y armonizados y condiciones de igualdad. El SEPD hace un llamamiento a la Comisión para que organice esta iniciativa.

84. Por último, aunque no por ello menos importante, tanto las autoridades nacionales como sus contrapartes europeas, incluido el ORECE y la Comisión Europea, deben prestar una mayor atención a la evolución del mercado en este ámbito. Desde el punto de vista de la protección de datos y la intimidad, un panorama en que los PSI aplican de manera rutinaria políticas de gestión del tráfico al ofrecer abonos basados en un acceso filtrado a los contenidos y las aplicaciones, resultaría muy problemático. Si esto ocurriera, sería necesario aplicar una legislación que solucionara dicha situación.

## VII. **CONCLUSIONES**

85. La creciente dependencia de los PSI en las técnicas de supervisión y de inspección vulnera la neutralidad de internet y la confidencialidad de las comunicaciones, lo cual plantea graves cuestiones relacionadas con la protección de los datos personales y la intimidad de los usuarios.

86. Aunque la Comunicación de la Comisión relativa a la internet abierta y la neutralidad de la red en Europa trata brevemente estas cuestiones, el SEPD opina que deberían darse más pasos para lograr una política satisfactoria. En el presente dictamen, el SEPD ha contribuido, por tanto, al debate político en curso sobre la neutralidad de la red, en especial respecto de los aspectos relativos a la protección de datos y la intimidad.

87. El SEPD considera que existe la necesidad de que las autoridades nacionales y el ORECE supervisen la situación del mercado. Dicha supervisión debería dar como resultado una imagen clara que describa si el mercado está evolucionando hacia una inspección masiva y en tiempo real de las comunicaciones y las cuestiones relacionadas con el cumplimiento del marco jurídico.

88. La supervisión del mercado no debería llevarse a cabo sin realizar un mayor análisis de los efectos de las nuevas prácticas relativas a la protección de datos y la intimidad en internet. El presente dictamen destaca algunos ámbitos que se beneficiarían de dicha aclaración. Aunque las agencias y organismos de la Unión como el ORECE, el Grupo de Trabajo del Artículo 29 y el SEPD pueden tener una buena posición para aclarar las condiciones de aplicación del marco, el SEPD considera que la Comisión tiene el deber de coordinar y dirigir el debate. Por lo tanto, el SEPD hace un llamamiento a la Comisión para que adopte una iniciativa que implique para dicho fin a todas las partes implicadas en una plataforma o grupo de trabajo. Entre las cuestiones que precisan un mayor análisis, deberán tratarse los siguientes puntos:

— determinar las prácticas de inspección que son legítimas para garantizar la fluidez del tráfico y que pueden llevarse a cabo con fines de seguridad;

— determinar cuándo la supervisión exige el consentimiento por parte de los particulares, en especial el consentimiento de todos los usuarios interesados, así como los parámetros técnicos permitidos para garantizar que la técnica de inspección no implica un tratamiento de datos desproporcionado para su finalidad;

— en los casos anteriores, puede ser necesaria una orientación relativa a la aplicación de las garantías necesarias de protección de datos (limitación a una finalidad específica, seguridad, etc.).

89. En función de las conclusiones, podrán ser necesarias medidas legislativas adicionales. En dicho caso, la Comisión debería presentar medidas políticas destinadas a reforzar el marco jurídico y garantizar la seguridad jurídica. Las nuevas medidas deberían aclarar las consecuencias prácticas del principio de neutralidad de la red, ya que esto ya ha sido llevado a cabo en algunos Estados miembros, así como garantizar que los usuarios pueden disponer de una elección real, en especial obligando a que los PSI ofrezcan conexiones no supervisadas.

Hecho en Bruselas, el 7 de octubre de 2011.

Peter HUSTINX

*Supervisor Europeo de Protección de Datos*