IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

www.uoc.edu/idp

ARTÍCULO

La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad

Mònica Vilasau

Resumen

La Directiva 2006/24/CE sobre la conservación de datos del tráfico en las comunicaciones electrónicas comporta un profundo cambio de los principios básicos de la protección de datos personales. Los proveedores de servicios de comunicaciones electrónicas deben conservar los datos que permitan identificar el origen, el destino, la fecha, hora y duración de una comunicación electrónica, el tipo de comunicación realizada, el equipo utilizado y la localización de dicho equipo.

Con ello se pretende garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves. Se concede a los Estados amplias facultades de control que han sido ampliamente criticadas por las instancias que velan por la adecuada protección de datos personales ya que supone contravenir los principios hasta el momento asentados sobre esta materia. Además, la redacción de la Directiva contiene una serie de imprecisiones que la hacen aún más criticable: indeterminación de los delitos que permitirán usar los datos, insuficiencia de las medidas de seguridad establecidas, indefinición del procedimiento para tener acceso a los datos y finalmente, silencio respecto a quién soportará los costes que comportan las medidas a adoptar.

Nos hallamos ante un instrumento que en aras de la seguridad sacrifica la privacidad de los ciudadanos sin que de entrada exista ningún indicio que permita sospechar de ellos.

Abstract

Directive 2006/24/EC on the retention of electronic communications traffic data involves a major change to the basic principles of personal data protection. Suppliers of electronic communication services must retain any data that reveal the origin, destination, date, time and length of an electronic communication, the type of communication carried out, the equipment used and its location.

The objective is to ensure that such data is made available for investigating, detecting and prosecuting serious offences. The broad faculties of control given to member States have been widely criticised by all institutions that monitor personal data protection, given that such faculties contravene the underlying principles that have been in place until now. Moreover, the Directive includes a number of ambiguities that make it even more open to criticism: it does not specify for which offences the data will be used, the established security measures are inadequate, the procedure for gaining access to the data has not been defined and, finally, no mention is made as to who will bear the cost of the measures to be adopted.

We are facing an instrument that sacrifices the privacy of citizens for the sake of security, without any prior evidence to warrant their being the target of suspicion.

Palabras clave
conservación de datos, comunicaciones electrónicas, privacidad, medidas de seguridad, acceso a los datos

Tema
Protección de datos

Keywords
data retention, electronic communications, privacy, security measures, access to the data

Topic
Data protection

Introducción

En la sociedad occidental se ha disparado la preocupación por la seguridad y la necesidad de dotar a los Estados de los máximos instrumentos para luchar contra el terrorismo. Entre estos instrumentos, se considera fundamental poder recurrir a la retención de datos del tráfico en las comunicaciones electrónicas. Así lo manifestó el Consejo europeo, en su declaración sobre la lucha contra el terrorismo, de 25 de marzo de 2004 y la misma idea se reiteró en las Conclusiones de la Presidencia, en junio de 2005.[1] Finalmente, el Consejo europeo de 13 de julio de 2005, en su sesión extraordinaria tras los atentados de Londres, declaró como una de sus prioridades la aprobación de una normativa sobre retención de datos.[2]

En este marco, la Comisión Europea presentó, el 21 de septiembre de 2005, una Propuesta de Directiva sobre conservación de datos del tráfico –en adelante la Propuesta-.[3] Esta Propuesta, que recibió duras críticas durante su tramitación, fue finalmente aprobada el 15 de marzo de 2006. Se trata de la Directiva 2006/24/CE del Parlamento europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.[4]

Nos hallamos ante un instrumento normativo de armonización de las legislaciones de los Estados miembros, que, con el objeto de investigar, detectar y enjuiciar determinados delitos graves establece obligaciones de almacenamiento y procesamiento de datos por parte de los proveedores de servicios de comunicaciones electrónicas públicas. Ya en el 2004, cuatro Estados miembros (Francia, Irlanda, Reino Unido y Suecia) presentaron un proyecto de decisión marco sobre el mismo tema (CNS/2004/0813), iniciativa que fue rechazada por el Parlamento Europeo.

1. Véase las Conclusiones de la Presidencia, Bruselas, 16 y 17 de junio de 2005 (http://ue.eu.int/ueDocs/cms_Data/docs/pressData/es/ec/85347.pdf). En el punto 19, al hacer referencia al espacio de libertad, seguridad y justicia, se declaraba que el Consejo Europeo deseaba que durante el segundo semestre de 2005 se abordaran con carácter prioritario una serie de puntos entre los que figuraba «los trabajos legislativos destinados a reforzar la cooperación policial y judicial, más concretamente y en la medida de lo posible en lo que atañe al intercambio de informaciones entre autoridades policiales, al exhorto de obtención de pruebas, a la retención de datos sobre tráfico de telecomunicaciones, así como al intercambio de información y a la cooperación sobre delitos de terrorismo».
2. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/es/jha/85826.pdf
3. Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE. {SEC(2005) 1131}. Bruselas, 21.9.2005, COM(2005) 438 final 2005/0182 (COD).
4. DO L 105 de 13.4.2006, pág. 54. http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/l_105/l_10520060413es00540063.pdf

Sin embargo, como afirma el profesor Rodotà, uno de los mayores especialistas sobre la materia, «no estamos discutiendo una Directiva sectorial. Nos enfrentamos a una verdadera redistribución de poder social, una redefinición de la posición de la persona y de la ciudadanía». Esta Directiva es uno de los ejemplos más claros del cambio de la lógica fundamentadora de la protección de datos personales que corre el riesgo de convertirse en el cuadro normativo del futuro.[5]

1. El proceso de aprobación de la Directiva

1.1. Razones de su adopción

La aprobación de esta Directiva obedece a distintas razones. En primer lugar, como ya se ha indicado, la finalidad de luchar contra el terrorismo y el crimen organizado en la medida que se considera la conservación de datos un elemento crucial para ello.

En segundo lugar la necesidad de adoptar disposiciones armonizadoras a nivel de la UE sobre retención de datos. La Directiva 2002/58/CE establece en sus arts. 5, 6 y 9 el principio general de la destrucción de los datos del tráfico (o su anonimización) cuando ya no se necesiten para la transmisión, a excepción de los datos necesarios para la facturación o los pagos por interconexión. El art. 15.1 dispone que los Estados miembros podrán prever excepciones a los anteriores artículos.

Al amparo de este último precepto, se han dictado algunas leyes por parte de los Estados miembros, que regulan la retención de datos, estableciéndose una tipología diversa tanto respecto de los datos a retener como de los plazos de retención. Se considera que la disparidad de legislaciones supone un obstáculo para el mercado interior de comunicaciones electrónicas y de ahí la necesidad de adoptar una Directiva sobre la materia.[6]

1.2. Instrumento jurídico utilizado

A la hora de determinar cuál era el instrumento más adecuado para regular la conservación de datos, se barajaron distintas opciones: no tomar ninguna medida, dejarlo a la autorregulación, adoptar una medida del tercer pilar o una del primer pilar. Esta última opción es la que se ha considerado más adecuada. Entre las razones que justifican su adopción, figura el hecho de que la conservación de datos de tráfico ya ha sido tratada en instrumentos legislativos previos sobre una base jurídica del primer pilar, especialmente por la Directiva 2002/58/CE. Se considera además que la fórmula de la Directiva, respecto del Reglamento, proporciona el nivel de armonización necesario a nivel comunitario y deja además a los Estados miembros un cierto margen de maniobra de cara a su implementación.[7]

1.3. Bienes jurídicos que están en juego

La adopción de una medida sobre retención de datos ha comportado la valoración de distintos intereses en juego contrapuestos. Frente al interés de las autoridades en la retención para luchar de forma más eficaz contra el terrorismo y otras formas de delincuencia organizada, se halla el derecho fundamental de los ciudadanos a la protección

5. RODOTÀ, Stefano (2006). «La conservación de los datos de tráfico en las comunicaciones electrónicas». En: «Segundo congreso sobre Internet, derecho y política: análisis y prospectiva» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política.* Nº. 3. UOC. http://www.uoc.edu/idp/3/dt/esp/rodota.pdf
6. Véase el documento de trabajo sobre la evaluación del impacto de la Propuesta de Directiva [Bruselas, 21.9.2005. SEC (2005) 1131]. En adelante: Documento de evaluación. http://ec.europa.eu/justice_home/doc_centre/police/doc/sec_2005_1131_en.pdf
7. Véase el documento de evaluación, pág. 9-11

sus datos. Además hay que añadir los intereses de los proveedores de servicios de comunicaciones electrónicas en que no les atribuyan más cargas económicas derivadas de las nuevas obligaciones.

Frente a los intereses de los Estados de poder retener los datos durante un período de tiempo cuanto más amplio mejor, y de retener cuantos más datos, los intereses de los ciudadanos pasan porque los plazos de retención sean lo más breves posibles, se retengan cuanto menos datos mejor y no se afecte al contenido de las comunicaciones (sobre este último aspecto volveremos más adelante ya que se trata de un arma de doble filo).

Los intereses de los proveedores de servicios de comunicaciones se juegan principalmente en dos aspectos: en que los períodos de conservación sean lo más breves posibles y en el del reembolso de los costes en que incurran.[8]

El documento de evaluación del impacto de la Propuesta de Directiva considera que la limitación de los derechos fundamentales en juego es proporcional y necesaria para alcanzar los objetivos de prevenir y luchar contra el terrorismo y el crimen organizado, teniendo en cuenta que se limita tanto la finalidad de la retención, el tipo de datos a retener y los plazos de retención. Además, la Directiva no resulta aplicable al contenido de las comunicaciones. Por otro lado, el tratamiento de los datos retenidos está sujeto a las garantías de las Directivas 95/46/CE y 2002/58/EC y por lo tanto bajo la supervisión de las autoridades de protección de datos.[9]

1.4. Polémica aprobación de la misma: opiniones desfavorables de las distintas instancias implicadas

La aprobación de esta Directiva no ha estado exenta de polémica y recibió duras críticas por parte del Grupo de trabajo del Artículo 29,[10] del supervisor europeo de protección de datos, del Parlamento y del Comité Económico y Social, siendo la principal objeción a la Propuesta el considerar que no se tutelaban suficientemente los Derechos fundamentales en juego.

El 26 de septiembre de 2005, el supervisor europeo de protección de datos (SEPD) aprobó su Dictamen en el que manifestaba no estar convencido de la necesidad de la retención de datos.[11] El SEPD considera que la medida adoptada no aporta una respuesta adecuada y proporcionada a las necesidades de la sociedad (véase el punto 26). Así mismo considera que la Propuesta no adopta las salvaguardias necesarias para tutelar suficientemente los derechos fundamentales en juego (véase los puntos 27 y 28).

Las conclusiones a las que llega son que debería insistirse en las medidas concretas respecto el acceso y la utilización posterior de los datos, garantizarse el ejercicio de los derechos de los titulares de los datos y añadir incentivos a

8. En cuanto a los costes, véase el documento de evaluación, págs. 15-20. El problema de los costes se plantea sobre todo respecto de las compañías pequeñas, ya que el establecimiento de las obligaciones de retención puede poner en peligro su supervivencia. En cualquier caso, el establecimiento de los datos concretos a retener también incide en unos mayores o menores costes. (En la Propuesta, la existencia de un anexo sobre los tipos de datos, que podía sujetarse a revisión, daba más flexibilidad a la hora de modificar y por lo tanto determinar la incidencia concreta respecto los costes. Sin embargo ello suponía sustraer la modificación del control del Parlamento y finalmente esta solución fue rechazada).
9. Véase el documento de evaluación, págs. 20-21
10. En cuanto a la creación del grupo del art. 29, su composición y cometido, vid. arts. 29 y 30 de la Directiva 95/46/CE.
11. Dictamen del Supervisor Europeo de Protección de Datos, adoptado el 26 de septiembre de 2005 (2005/C 298/01), sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la retención de los datos procesados en conexión con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005) 438 final]. DO C 298 de 29.11.2005, pág. 1. http://eur-lex.europa.eu/LexUriServ/site/es/oj/2005/c_298/c_29820051129es00010012.pdf

los proveedores para que inviertan en una infraestructura técnica adecuada. Muchas de sus recomendaciones no han sido tenidas en cuenta, por ejemplo el acceso a los datos no ha sido suficientemente regulado y se ha dejado por completo a la implementación por parte de cada Estado. Tampoco se ha hecho ninguna mención a los costes –con lo que supone de desincentivo a la adopción de medidas de seguridad– ni se ha concretado la destrucción de los datos.

El 21 de octubre de 2005 el Grupo del Artículo 29 en su Dictamen sobre la Propuesta de Directiva (WP 113) declaraba que ésta «nos enfrenta a una decisión histórica».[12] Las conclusiones a las que llega el Grupo de trabajo en el WP 113 son que la justificación para la conservación obligatoria y general de los datos debe demostrarse claramente y apoyarse con pruebas.[13] Esto se aplica también a los períodos máximos de retención. Finalmente, el Grupo de trabajo propone establecer veinte garantías específicas, prestando especial atención a los requisitos aplicables a los destinatarios y al tratamiento posterior de los datos, a la importancia de las autorizaciones y controles, a las medidas aplicables a los prestadores de servicios, a la determinación de las categorías de datos en cuestión y su actualización, y a la necesidad de excluir datos relativos al contenido.

El Parlamento europeo también fue crítico con la Propuesta y aprobó una serie de enmiendas que trataban de tutelar los derechos de los titulares de los datos. Por ejemplo, la enmienda 82, que introduce un nuevo artículo 7 Bis que se convertirá en el art. 7 del texto definitivo y que supone poner más énfasis en la necesidad de adoptar medidas de seguridad. O bien la enmienda 88, que introduce un nuevo artículo 11 Ter que se convertirá en el art. 13 del texto definitivo y que hace referencia a los recursos judiciales, responsabilidades y sanciones.

Sin embargo el Parlamento europeo también adoptó algunas enmiendas más discutibles, como la enmienda 85, que suprime el art. 10 de la Propuesta que hacía referencia a los costes o la enmienda 87 que propone la introducción de un nuevo artículo 11 bis, que se convierte en el art. 12 del texto definitivo, relativo a las medidas futuras y a las que haremos referencia.[14]

El 19 de enero 2006, el Comité Económico y Social Europeo (CESE) aprueba el dictamen relativo a la Propuesta. Según sus propias palabras, «manifiesta su extrañeza y preocupación» por la misma en la medida que no se da un tratamiento adecuado al derecho a la intimidad. Además señala el riesgo que supone socavar la confianza de los usuarios en las comunicaciones electrónicas (frenar el desarrollo de la sociedad de la información) y discrepa de la solución de la Propuesta relativa a quién debe soportar los costes adicionales en los que incurren los operadores. La conclusión del CESE es que debe revisarse sustancialmente la Propuesta, en la medida en que no respeta en su totalidad los derechos fundamentales ni las reglas de acceso, uso e intercambio de los datos (véase punto 2.4.15).[15]

12. Dictamen 4/2005, adoptado el 21 de octubre de 2005 (1868/05/ES. WP 113), sobre la Propuesta de Directiva sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005)438 final de 21.09.2005]. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_es.pdf
13. En cambio, en el documento de evaluación, pág. 3-5 se considera que la conveniencia y necesidad de la retención de datos está suficientemente justificada.
14. Véase respecto todas las enmiendas la resolución legislativa del Parlamento europeo de 14 de diciembre de 2005 sobre la Propuesta de directiva del Parlamento europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE [COM(2005)0438 – C6-0293/2005 – 2005/0182(COD)].
15. Dictamen del Comité Económico y Social Europeo, de 19 de enero 2006, sobre la «Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la conservación de datos tratados en relación con la prestación de servicios públicos de comunicación electrónica y por la que se modifica la Directiva 2002/58/CE» COM(2005) 438 final — 2005/0182 (COD). (2006/C 69/04). DO C 69 de 21.3.2006, pág. 16. http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/c_069/c_06920060321es00160021.pdf

El 25 de marzo 2006, con posterioridad a la aprobación de la Directiva, el Grupo del Artículo 29 emitió el Dictamen 3/2006 relativo a su aplicación (WP 119). Dicho grupo declara de nuevo su preocupación por las previsiones contempladas en la Directiva y reitera su opinión de octubre del 2005. Considera que esta Directiva debe acompañarse de medidas que aminoren el fuerte impacto sobre la privacidad.[16]

En concreto, el Grupo del Artículo 29, en la medida que considera que la Directiva carece de algunas salvaguardas específicas, propone una aplicación armonizadora de sus preceptos y recomienda la adopción de determinadas medidas. Entre ellas cabe destacar la necesidad de determinar claramente qué se entiende por «delitos graves», la prohibición de *datamining*, la prohibición de procesar los datos retenidos por parte de los proveedores de servicios o bien una mayor delimitación de las medidas de seguridad necesarias.

2. Contenido de la Directiva 2006/24/CE

2.1. Objetivo

La Directiva 2006/24/CE se propone armonizar las disposiciones de los Estados miembros relativas a las obligaciones de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones en relación con la conservación de determinados datos generados[17] o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento[18] de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro. (Art. 1.1.).

El art. 1.2 establece que la presente Directiva se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o al usuario registrado. No se aplicará al contenido de las comunicaciones electrónicas, lo que incluye la información consultada utilizando una red de comunicaciones electrónicas.

Esta obligación de conservación de los datos supone una excepción a los arts. 5, 6 y 9 de la Directiva 2002/58/CE.

La primera objeción que se hace a la finalidad de la Directiva 2006/24 es que las medidas adoptadas son extremadamente vulneradoras de los derechos fundamentales de los ciudadanos y que existen otros mecanismos menos invasores. Uno de ellos es el denominado *quick freeze*, en cuyo caso no se lleva a cabo un almacenamiento general de los datos sino que en casos justificados las autoridades policiales piden a los proveedores que almacenen ciertos datos y posteriormente pueden obtener una orden judicial que les permita acceder a los mismos.[19]

16. Dictamen 3/2006, adoptado el 25 de marzo de 2006 (654/06/ES. WP 119) sobre la Directiva 2006/24/CE del Parlamento Europeo y del Consejo sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, adoptada por el Consejo el 21 de febrero de 2006. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_es.pdf

17. Tanto el título de la Propuesta de Directiva de 21.9.2005, como el artículo 1.1. de dicha Propuesta, hacían referencia sólo a datos «tratados», sin contemplar los datos «generados» en relación con la prestación de servicios públicos de comunicación electrónica, por lo que el ámbito de aplicación del texto definitivamente aprobado puede parecer más amplio que el de la Propuesta. Sin embargo, el artículo 3.1. de la Propuesta, al hacer referencia a la obligación de conservar datos, contemplaba tanto los datos «tratados» como los «generados».

18. El art. 1.1. de la Propuesta de directiva hacía referencia a: prevención, investigación, detección y enjuiciamiento. En el texto definitivo se ha suprimido la finalidad de «prevención»

19. En este sentido se pronuncia el Grupo del Artículo 29, véase. WP 113, pág. 7.

El art. 1.1. de la Propuesta de Directiva al hacer referencia a «delitos graves» especificaba «como el terrorismo y la delincuencia organizada»,[20] sin embargo, el texto definitivamente aprobado ha suprimido esta concreción. El Grupo del Artículo 29 consideraba que «los datos sólo deberán conservarse con el fin específico de luchar contra el terrorismo y la delincuencia organizada, en vez de considerarse cualesquiera otras «infracciones graves» indeterminadas. Según dicho grupo, la limitación de la finalidad también debería figurar en el título de la Directiva Propuesta (WP 113, pág. 9). En vista del texto definitivamente adoptado el Grupo del Artículo 29 propone una transposición del mismo de forma que el término «infracciones graves» quede claramente definido y no sean posibles interpretaciones extensivas (WP 119, pág. 3).

2.2. Sujetos afectados

Los sujetos obligados a retener los datos son los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones.

Los datos se retienen respecto de personas físicas y jurídicas (art. 1.2 Directiva). Así lo confirma el art. 2.2.b) cuando se refiere al «usuario» como toda persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público.

Al definir al «usuario» a los efectos de la Directiva, el art. 2.2. b) realiza otra precisión. Entiende por «usuario» la persona física o jurídica que utilice un servicio de comunicaciones electrónicas de acceso público,con *fines privados o comerciales*, sin haberse necesariamente abonado a dicho servicio.

Esta referencia a *fines privados o comerciales* ¿comporta que se excluya del concepto de usuario para la aplicación de la Directiva a la Administración pública?

En el art. 1.2. no parece contemplarse esta exclusión, pero el interrogante se plantea a tenor del art. 2.2.b). Sin embargo, esta exclusión no tendría mucho sentido. Como veremos más adelante, entre los datos del tráfico que se retienen se hallan los necesarios para «identificar el destino de una comunicación» [art. 5.1.b)]. En el caso de excluir de la obligación de retener los datos del tráfico relativos a la administración, ello afectaría no sólo a los datos que genera la propia administración en las comunicaciones entre sus órganos o con otras administraciones, sino también aquellos otros supuestos en que la Administración se relaciona con terceros (como receptora u origen de una comunicación).[21]

Los sujetos que pueden ser destinatarios de los datos son *solamente* las «autoridades nacionales competentes» (art. 4 y 8). En parecidos términos se pronunciaban los arts. 3.2 y 8 de la Propuesta. Con el término *solamente* se pretende dejar claro, siguiendo los comentarios del SEPD, que otras personas distintas de las autoridades competentes no puedan tener acceso a los datos en cuestión (Dictamen del SEPD, punto 52). De todas formas hubiera sido necesario precisarlo más.

El Grupo del Artículo 29 consideraba, respecto de la Propuesta, que debería establecerse que «los datos sólo estarán disponibles para determinadas autoridades policiales específicamente designadas cuando sea necesario a efectos de la investigación, detección, procesamiento y/o prevención del terrorismo. Deberá publicarse la lista de estas

20. También realizaba la misma puntualización el art. 11 de la Propuesta.
21. Por lo tanto, si se considera tan importante retener los datos respecto de un hipotético criminal, se desconocerían aquellos datos en los que el sujeto en cuestión se ha relacionado con la Administración. Si se predica que es tan indispensable poder retener los datos, no se justifica suficientemente que este supuesto quede excluido.
Además respecto a las administraciones, una parte de las comunicaciones que realizan los funcionarios y resto de personal (telefonía, acceso a Internet), afecta a la esfera privada. ¿Cómo se podría separar y controlar esta actividad distinta de la propia de la Administración?

autoridades» (WP 113, pág. 9). El Grupo del Artículo 29, en el Dictamen posterior a la aprobación de la Directiva, vuelve a reiterar la idea de la necesidad de hacer pública una relación de las autoridades designadas que puedan tener acceso a los datos (WP 119, pág. 3).

2.3. ¿Qué es objeto de conservación?

Los datos que son objeto de conservación son los datos de tráfico y de localización sobre personas físicas y jurídicas y los datos relacionados necesarios para identificar al abonado o al usuario registrado. En cambio, no se aplica la Directiva al contenido de las comunicaciones electrónicas (art. 1.2).[22]

El art. 5 establece de forma más pormenorizada las categorías de datos que serán objeto de conservación. Los datos necesarios para: i) rastrear e identificar el origen de una comunicación; ii) identificar el destino de una comunicación; iii) identificar la fecha, hora y duración de una comunicación; iv) identificar el tipo de comunicación; v) identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación; vi) identificar la localización del equipo de comunicación móvil.

El art. 4 de la Propuesta recogía una relación similar de datos pero establecía una variante en cuanto a la forma. El art. 4 únicamente hacía una relación general de los datos y luego se remitía a un anexo que desgranaba cada uno de los datos dentro de las categorías previamente establecidas. Dicho anexo sería objeto de revisión regularmente, en la medida que fuera necesario, de acuerdo con el procedimiento establecido en el art. 6 de la Propuesta –la Comisión, asistida por un Comité, revisaría dicho anexo.

El Grupo del Artículo 29 no consideró adecuada la mecánica de remitir a un anexo la relación concreta de datos a retener. Por el contrario, consideraba que la propia Directiva debía especificar directamente la lista de datos personales a conservar. Y ello para poder calibrar exactamente el impacto en los derechos y libertades fundamentales de los ciudadanos afectados, teniendo en cuenta los riesgos para su esfera personal y la garantía de la exactitud y la actualización de los datos conservados.

Asimismo, consideraba que toda propuesta de cambios en la lista de los tipos de datos a conservar debería someterse a una prueba de estricta necesidad. Por ello, la revisión de dicha lista debería realizarse sólo con la aprobación del Parlamento europeo y con la participación de las autoridades responsables de protección de datos. En consecuencia, se consideraba inadecuado realizar la revisión de dicha lista únicamente siguiendo el procedimiento de comitología, según lo previsto en la Propuesta de Directiva (WP 113, págs. 10-11). El mismo parecer expresó el SEPD, punto 60.

El Parlamento europeo también se pronunció en un sentido parecido, señalando que no era correcto establecer en un anexo los datos a retener, ya que era un tema sobre el que necesariamente debía pronunciarse el propio Parlamento y no se podía dejar a la Comisión.[23] El CESE, punto 2.4.6, expresó la misma opinión.

22. En el mismo sentido se pronuncia el art. 2.2.a) Directiva cuando determina qué se entiende por *dato* a los efectos de la aplicación de la misma. El art. 5.2 reitera que «no podrá conservarse ningún dato que revele el contenido de la comunicación». Esta medida, si bien de entrada puede parecer positiva, tiene el inconveniente del efecto boomerang del que habla el profesor Rodotà «si se realiza una llamada telefónica inocente a quien luego se revela un criminal, la imposibilidad de demostrar cuál ha sido el verdadero contenido de la comunicación dejará la sombra de la sospecha.». (*Vid.* Rodotà, op. *cit.*).

Finalmente el texto definitivo ha seguido las opiniones emitidas y en el art. 5 se incluye la relación detallada de los datos a conservar.

2.4. Circunstancias que rodean la conservación de datos

2.4.1. Conservación y almacenamiento

Una vez que los datos han sido retenidos, el primer elemento a tener en cuenta es cómo se produce la conservación y almacenamiento de los mismos. El art. 3.1 de la Propuesta establecía que los datos «se conserven de conformidad con lo dispuesto en la presente Directiva». Sin embargo, en el resto del articulado no se hacían ulteriores referencias a las garantías de los titulares de los datos.

Esta falta de concreción fue criticada por las autoridades de protección de datos. El Grupo del Artículo 29 consideraba que «las medidas comunitarias deberán prever normas mínimas sobre medidas de seguridad técnicas y organizativas que deberán adoptar los proveedores, especificando los requisitos generales relativos a las medidas de seguridad establecidas en la Directiva CE/2002/58 (WP 113, pág. 10).

Pues bien, la Directiva, a parte de una declaración general contenida en el art. 3.1 de que los datos se deberán conservar de conformidad con lo dispuesto en la Directiva, sí que introduce un precepto que, si bien de forma muy general, se refiere a la protección y seguridad de los datos. Se trata del art. 7 que se ocupa de las garantías de los titulares de los datos (calidad, normas de seguridad, acceso y destrucción). Pero el Grupo del Artículo 29 indica la necesidad de especificar en las legislaciones nacionales, las medidas de seguridad, estableciendo unos estándares mínimos, especificando los requisitos generales sentados en la Directiva (WP 119, pág. 3).

Pero el interés de la Directiva parece focalizarse en otro aspecto. En su articulado, aparte de hacer una referencia a las medidas de seguridad, se preocupa de tutelar y garantizar otro interés: el de las autoridades receptoras de los datos. En consecuencia el art. 8 establece que los datos deben conservarse de tal forma que puedan transmitirse sin demora cuando las autoridades competentes así lo soliciten.

En términos muy parecidos se pronunciaba el art. 8 de la Propuesta y además, en dicha Propuesta no existía ninguna mención a las garantías de los titulares de los datos. Resulta preocupante que el principal objetivo de la conservación adecuada fuera facilitar el acceso a los datos a las autoridades y no el de garantizar los derechos de los afectados. Si bien este aspecto se ha corregido un poco en el texto definitivo, es revelador de la filosofía que late bajo la Directiva.[24]

2.4.2. Acceso a los datos

El art. 3.2 de la Propuesta establecía, en términos bastante parecidos al artículo 4 de la Directiva, la necesidad de adoptar medidas para garantizar que los datos conservados de acuerdo con la Directiva solamente se propor-

23. En este sentido se pronunció la Comisión de Industria, Investigación y Energía, que en las enmiendas n.º 18, 19 y 20 propuso sumprimir los arts. 4.2, 5 y 6 de la Propuesta de directiva. Véase http://www.europarl.europa.eu/omk/sipade3?PUBREF=-//EP//NONSGML+REPORT+A6-2005-0365+0+DOC+PDF+V0//ES&L=ES&LEVEL=2&NAV=S&LSTDOC=Y, pág. 40-41 y 50-51
Según su parecer, «no puede aceptarse el procedimiento de comitología propuesto por la Comisión, en cuyo seno los representantes de la Comisión y de los Estados miembros podrán modificar la lista de los datos que deben conservarse sin la participación del Parlamento europeo y las empresas concernidas. Cada ampliación de los tipos de datos que deben conservarse tiene una incidencia clara en los derechos fundamentales y debe someterse a la consideración del Parlamento. Por tanto, debe suprimirse este artículo».

24. El SEPD, en el punto 62, junto a otras consideraciones relativas a la transmisión de los datos (no revelar otros datos distintos de los datos necesarios a efectos de la solicitud), afirmaba que «los proveedores deben instalar el entramado técnico necesario, incluidos motores de búsqueda, para facilitar el acceso directo a los datos específicos». ¿Realmente esta última medida supone una tutela de los ciudadanos?

cionen a las autoridades nacionales competentes y, en casos específicos, de conformidad con la legislación nacional, con fines de prevención, investigación, detección y enjuiciamiento de delitos graves, como el terrorismo y la delincuencia organizada.[25]

Como ya se ha señalado anteriormente al hablar de los destinatarios de los datos, una de las críticas a dicha redacción era la excesiva generalidad del término «autoridades nacionales competentes», indicando tanto el SEPD como el Grupo del Artículo 29 la necesidad de que las legislaciones nacionales identificaran claramente cuáles eran las autoridades en cuestión.

El SEPD consideraba necesario adoptar una serie de previsiones en cuanto al acceso a los datos: regular de forma más detallada el intercambio de datos entre autoridades de distintos Estados (punto 32), regular explícitamente el acceso y la utilización posterior de los datos (punto 50), especificar que los datos sólo pueden proporcionarse cuando sea necesario en relación con una infracción penal concreta, y no para búsquedas aleatorias (punto 53) y establecer que el acceso en casos específicos debería estar supeditado al control judicial en los Estados miembros (punto 56). El Dictamen del CESE va en la misma dirección y considera que el acceso a los datos debería realizarse sólo en casos específicos y bajo control judicial (punto 2.4.9).

Ahondando más en el acceso a los datos, el Grupo del Artículo 29 considera que «el acceso a los datos deberá, en principio, autorizarse debidamente en cada caso por una autoridad judicial, sin perjuicio de los países donde exista la posibilidad específica de acceso autorizado por ley, bajo supervisión independiente. En su caso, las autorizaciones deberán especificar los datos particulares requeridos para los casos concretos (WP 113, pág. 10 y WP 119, pág. 3). También consideraba el Grupo del Artículo 29 la necesidad de registrar todo acceso a los datos (WP 113, pág. 10).

Pese a estas observaciones, la Directiva simplemente se limita a introducir un nuevo párrafo (el art. 4.2) que deja a los Estados miembros la definición del procedimiento a seguir y las condiciones que deban cumplirse para tener acceso a los datos. «Cada Estado miembro definirá en su legislación nacional el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad, de conformidad con las disposiciones pertinentes del derecho de la Unión o del derecho internacional público, y en particular el CEDH en la interpretación del Tribunal Europeo de Derechos Humanos».

2.4.3. Plazo de conservación

A la hora de determinar el plazo que deben conservarse los datos nos hallamos ante el interés de las autoridades de garantizar un período suficientemente amplio y por el otro el de los titulares de los datos y de las empresas en que los plazos sean cuanto más breves mejor.

El art. 6 de la Directiva establece que las categorías de datos mencionadas en el art. 5 se conserven por un período de tiempo que no sea inferior a seis meses ni superior a dos años a partir de la fecha de la comunicación, sin distinguir al establecer dichos plazos, el tipo de dato de que se trate.

25. El final de este artículo de la Propuesta, en concreto cuando hace referencia a «con fines de prevención [....] terrorismo y la delincuencia organizada.», se ha suprimido en su equivalente, el art. 4.1 de la directiva. Pese a que puede parecer una coletilla sin trascendencia, era positivo que se reiterara en qué casos concretos se podía tener acceso a los datos. Esta supresión del texto actual del art. 4.1 hay que ponerla en relación con el hecho de que en el propio art. 1 de la directiva se hace referencia a «delitos graves», sin especificar cuáles son.

Por contra el art. 7 de la Propuesta establecía un plazo general de conservación de un año y uno más reducido de 6 meses para los datos relacionados con comunicaciones electrónicas que tuvieran lugar entera o principalmente a través del protocolo Internet.[26]

En el texto de la Directiva, si bien no se tiene en cuenta la circunstancia del tipo de dato para establecer los plazos de conservación, esta circunstancia sí que se valora al regular la transposición de la Directiva. El art. 15 establece la posibilidad de que los Estados miembros aplacen durante un año y medio la aplicación de la Directiva respecto la conservación de los datos de comunicaciones a través de Internet.

La Propuesta de Directiva no hacía ninguna referencia a la obligación de borrar los datos al final del plazo de retención ni tampoco al procedimiento a seguir para llevarlo a cabo.[27] La Directiva contiene una referencia genérica, en el art. 7d), a que «los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación».

2.5. Aplicación de la Directiva

La presente Directiva, que entró en vigor el 3 de mayo del 2006 (vid. art. 16), deberá transponerse por los Estados miembros a más tardar el 15 de setiembre de 2007. Como ya se ha indicado, cada Estado miembro tenía la posibilidad de decidir, en el momento de adopción de la Directiva, aplazar hasta el 15 de marzo de 2009 la aplicación de la misma en lo que se refiere a la conservación de los datos de comunicaciones a través de Internet (acceso a Internet, telefonía por Internet y el correo electrónico).[28] Sin embargo, esta moratoria no será aplicable al caso de España, ya que no ha realizado ninguna declaración al respecto.[29]

Una de las novedades de la Directiva, respecto de la Propuesta, es la necesidad de que los Estados miembros nombren una autoridad pública responsable de controlar la aplicación de la Directiva en relación con la seguridad de los datos (art. 9). Dichas autoridades, que actuarán con plena independencia, pueden ser las Agencias de protección de datos ya existentes. Es lógico que se haya introducido este precepto en el texto definitivo en paralelo a la introducción de las referencias a las medidas de seguridad.

2.5.1. Estadística y evaluación

El art. 10 establece que los Estados miembros velarán por que se faciliten anualmente a la Comisión las estadísticas sobre la conservación de datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones. Tales estadísticas incluirán los casos en que se haya facilitado información a las autoridades competentes, el tiempo transcurrido entre la fecha en que se conservaron los datos y la fecha en que la autoridad competente solicitó su transmisión, y los casos en que no pudieron satisfacerse las solicitudes de datos. Tales estadísticas no contendrán

26. El SEPD considera adecuado tanto los plazos previstos por la Propuesta como establecer distintos plazos en función del dato a retener (véase el Dictamen del SEPD, puntos 61-62). Por el contrario, el Dictamen del CESE considera que el plazo de un año previsto en la Propuesta es demasiado largo, ya que la Comisión no acredita la necesidad de la retención por esos periodos. El Comité considera que un periodo prudencial y unificado debería ser el de seis meses, con las medidas de seguridad y confidencialidad adecuadas (véase el punto 2.4.8).
27. Véase en este sentido las observaciones del SEPD, punto 62.
28. Esta posibilidad prevista en el art. 15.3 de la Directiva de aplazar su aplicación respecto la conservación de datos transmitidos a través de Internet no estaba contemplada en la Propuesta de Directiva. Ello es en parte lógico ya que la Propuesta contemplaba un plazo distinto de retención (más breve) para los datos relacionados con comunicaciones electrónicas que tuvieran lugar entera o principalmente a través del Protocolo Internet –art. 7 de la Propuesta. En el texto definitivo no se prevé esta distinción.
29. Véase las declaraciones que constan al final del texto de la Directiva.

datos personales. En términos muy parecidos se pronunciaba el art. 9 de la Propuesta.

Estas estadísticas tienen como finalidad permitir una evaluación de la implantación de la Directiva. El art. 14 establece que tres años después de la transposición de la Directiva se presentará al Parlamento y al Consejo una evaluación de su aplicación y su impacto en operadores económicos y consumidores. Uno de los elementos a tener en cuenta para realizar esta evaluación serán las estadísticas mencionadas en el art. 10. Dicha evaluación tendrá como finalidad principal determinar si es necesario modificar las disposiciones de la Directiva en cuestión, especialmente la relación de datos a conservar y los períodos de conservación.

El art. 12 de la Propuesta tenía un contenido muy similar, con la diferencia de que lo que se planteaba evaluar era principalmente los períodos de conservación. (En cuanto a los tipos de datos, como ya se ha indicado, su revisión tenía un régimen específico ya que se dejaba a manos de una Comisión –arts. 5 y 6 de la Propuesta).

2.5.2. Responsabilidades y sanciones

A diferencia de la Propuesta, se hace una referencia expresa a la necesidad de que los Estados miembros adopten medidas para impedir accesos no debidos a los datos conservados y transferencias no permitidas por la legislación nacional, estableciendo las correspondientes sanciones administrativas o penales en caso de contravenir las normas previstas (art. 13).

2.5.3. Costes

Uno de los temas clave en la elaboración de la Directiva ha sido el de quién debía hacer frente a los costes que comporta su aplicación.[30] El artículo 10 de la Propuesta expresamente daba una respuesta al respecto y establecía que «los Estados miembros asegurarán que los proveedores de servicios de comunicación electrónica de acceso público o de una red de comunicaciones pública sean reembolsados por los costes adicionales en que demuestren haber incurrido para cumplir con las obligaciones que la presente Directiva les impone».

El SEPD subrayó la relación entre quién debe soportar los costes y la adopción de las medidas de seguridad adecuadas y consideraba positivo el reembolso de los costes previsto en la Propuesta de Directiva (punto 36, y puntos 67-70).

Por su parte, el Grupo del Artículo 29 en el WP 113 consideró que los gastos adicionales que soporten los proveedores de comunicaciones electrónicas deberán ser compensados por los Estados miembros. Según dicho grupo, debe darse una solución adecuada, de modo que no se produzcan efectos negativos en el nivel de protección de datos ni tampoco en la esfera económica de los ciudadanos, a quines se podría cargar parte de los gastos de los proveedores. Según el Grupo de trabajo, las medidas de conservación de datos deberán incluir el reembolso de las inversiones de adaptación de los sistemas de comunicaciones, de los gastos de la revelación de datos a las autoridades policiales y de las medidas de seguridad (WP 113, pág. 11-12).

Por el contrario, el Comité Económico y Social, en su Dictamen de 19 de enero de 2006, discrepaba totalmente de la previsión de la Propuesta de Directiva de reembolsar a los proveedores y consideraba que dichos costes debían contemplarse como «una carga que los operadores deberían asumir por el mero hecho de estar en el

30. Al respecto es interesante leer el documento de evaluación, págs. 14-20. Entre otros aspectos, el tema de los costes está relacionado con la duración de los plazos de conservación y los tipos de datos a retener. (Cuanto más tiempo y cuantos más datos a retener, más costes.)

mercado, sin que el erario público, y por ende todos los ciudadanos, tengan que soportarla».[31]

En el texto definitivo, se ha omitido toda referencia a la cuestión de los costes. La enmienda 85 del Parlamento propuso suprimir el art. 10 de la Propuesta que se pronunciaba en el sentido ya visto.[32] Ante el silencio de la Directiva sobre los costes, éste será el caballo de batalla a la hora de transponerla. Los Estados podrán pronunciarse en un sentido u otro (determinar que se reembolsará a los proveedores de servicios o que no será así). Como hemos visto, ello va muy ligado a las medidas de seguridad. Si efectivamente son los operadores quienes tienen que hacer frente a estos costes, las medidas de seguridad que se adopten probablemente no serán lo apropiadas y necesarias que deberían ser. En cualquier caso, parece que acabará pagándolo el propio usuario.

Pero además, no pronunciarse sobre los costes puede producir otro efecto negativo. Se alegaba, para justificar la adopción de la Directiva que «las diferencias en las disposiciones legislativas, reglamentarias y técnicas en los Estados miembros en materia de conservación de datos de tráfico plantean obstáculos para el mercado interior de comunicaciones electrónicas ya que los prestadores de servicios se enfrentan a requisitos diferentes en cuanto a los tipos de datos que deben conservarse».[33] Pues bien, el objetivo de unificación puede diluirse en la medida en que se deja a los Estados adoptar la solución que consideren más conveniente respecto al reembolso.

2.5.4. Medidas futuras

Donde se demuestra de forma más clara la amenaza que representa la Directiva es en el art. 12, que lleva por rúbrica: «medidas futuras». Este precepto no tenía ningún precedente en la Propuesta de Directiva. Su introducción es debida a la Enmienda 87 del Parlamento que propone la incorporación de un nuevo artículo, el 11 bis, que se convertirá en el art. 12 del texto definitivo.

Este precepto dispone que «(t)odo Estado miembro que deba hacer frente a circunstancias especiales que justifiquen una ampliación limitada del período máximo de conservación recogido en el artículo 6 podrá adoptar las medidas que se impongan. El Estado miembro en cuestión informará inmediatamente a la Comisión y a los demás Estados miembros sobre las medidas adoptadas de conformidad con el presente artículo e indicará las razones que le llevan a adoptarlas» (art. 12.1).

El art. 12.2. prevé que «(e)n un plazo de seis meses tras la notificación mencionada en el apartado 1, la Comisión aprobará o rechazará las medidas nacionales en cuestión después de haber examinado si constituyen una discriminación arbitraria o una restricción encubierta al comercio entre los Estados miembros o constituyen un obstáculo para el funcionamiento del mercado interior. En caso de que la Comisión no adopte ninguna decisión en dicho plazo se considerará que las medidas nacionales han sido aprobadas».

31. En relación con el tema de los costes, véase el Dictamen del CESE, puntos 2.4.11 a 2.4.14 en que se concluye que la Propuesta de reembolso de costes resulta improcedente y debe suprimirse. Sin embargo este punto del Dictamen fue objeto de fuerte controversia en el seno del CESE; véase el anexo al mismo donde se encuentran las Propuestas de enmiendas al Dictamen y el resultado de las votaciones.
32. Resolución legislativa del Parlamento europeo, cit.
33. Véase Exposición de motivos de la Propuesta, pág. 2, y Considerando 6 de la Directiva.

Se confiere pues al Estado unas amplias prerrogativas y parece que las críticas que se hicieron a la Propuesta de Directiva en lugar de suavizar las medidas adoptadas inicialmente han ampliado las facultades de retención. Este precepto permite ir aún más allá de las facultades previstas originariamente.

La interpretación del art. 12 plantea una duda principal, que es la del momento en que resultan aplicables las medidas aprobadas. ¿Tras su adopción por el Estado miembro o bien cuando la Comisión las aprueba –expresamente o mediante silencio positivo?

Puede parecer que no son directamente aplicables ya que el art. 12.2 establece que la Comisión «aprobará o rechazará las medidas nacionales» tras examinarlas. Sin embargo plantea confusión la interpretación de la frase «podrá adoptar las medidas que se impongan» –art. 12.1.[34]

Debería quedar más claro que las medidas no podrán aplicarse hasta que no conste la aprobación de la Comisión o bien transcurran seis meses sin que esta se pronuncie.

Existen aspectos criticables del artículo 12: el término «circunstancias especiales» es demasiado genérico y puede dar lugar a arbitrariedad y el hecho de que se puedan aprobar dichas medidas por silencio positivo resulta preocupante.

Otra objeción que puede hacerse a este precepto es que mediante el mecanismo en él previsto se producirá una modificación de la Directiva sin la intervención del Parlamento. Si una de las críticas a la Propuesta era que dejaba la determinación de los datos a retener al sistema de «comitología», en el art. 12 se incurre en el mismo error. Es cierto que se intenta corregir de alguna forma mediante el art. 12.3 que establece que cuando las medidas nacionales adoptadas por un Estado miembro se aparten de las disposiciones de la presente Directiva, la Comisión examinará la oportunidad de proponer la modificación de la presente Directiva. Sin embargo, mientras tal modificación no se produzca, las medidas ya se estarán aplicando.

Además este precepto choca frontalmente con algunas de las observaciones y recomendaciones que se habían establecido en relación con la Propuesta de Directiva. Así, el Dictamen del Grupo del Artículo 29 establecía que «deberá quedar claro que los Estados miembros no tendrán que establecer períodos de conservación de datos más largos que los previstos en la Directiva, aunque tendrán libertad para establecer períodos de conservación más breves», (WP 113, pág. 8). Mediante el art. 12 se está permitiendo lo que el Grupo del Artículo 29 trataba de evitar.

Resulta un poco extraño que el Grupo del Artículo 29, en el WP 119 adoptado con posterioridad a la aprobación de la Directiva, no haga ninguna referencia ni alerta sobre el precepto en cuestión.

Conclusiones

La conservación de los datos del tráfico interfiere con el derecho fundamental e inviolable a la confidencialidad de las comunicaciones y a la protección de datos.

34. La versión inglesa de la Directiva que quizá puede esclarecer el redactado del art. 12.1 establece: «12.1. A Member State facing particular circumstances that warrant an extension for a limited period of the maximum retention period referred to in Article 6 *may take the necessary measures*. That Member State shall immediately notify the Commission and inform the other Member States of the measures taken under this Article and shall state the grounds for introducing them» (la cursiva es nuestra). Parece que nos hallamos ante una de las cláusulas de salvaguardia previstas en el art. 95.10 TCE.

Mediante la Directiva 2006/24 se están socabando los principios de protección de datos sentados en la UE. En definitiva, las medidas adoptadas en la presente Directiva superan totalmente los beneficios que se puedan obtener con la misma ya que se instaura una filosofía de sospecha y vigilancia de todos los ciudadanos sin un mínimo indicio. Además, ya de forma directa, ya indirecta, son los propios usuarios quienes acabarán soportando los costes de las medidas adoptadas.

En cualquier caso, siguiendo las directrices del Grupo del Artículo 29 (WP 119), es de desear que la transposición de la Directiva por parte de los Estados se haga respetando al máximo los derechos de los ciudadanos reconocidos en los propios textos constitucionales y jurisprudencia interna que se convertirá en su última garantía.

Cita recomendada

VILASAU, Mònica (2006). «La Directiva 2006/24/CE sobre conservación de datos del tráfico en las comunicaciones electrónicas: seguridad v. privacidad» [artículo en línea]. *IDP. Revista de Internet, Derecho y Política*. Nº. 3. UOC. [Fecha de consulta: dd/mm/aa].
<http://www.uoc.edu/idp/3/dt/esp/vilasau.pdf>
ISSN 1699-8154

Mònica Vilasau

mvilasau@uoc.edu

Profesora de Derecho civil de la UOC. Ha publicado diversos trabajos sobre la responsabilidad en la construcción. En la actualidad su línea de investigación es la protección del derecho a la intimidad en relación con el uso de las tecnologías de la información y comunicación. Participa en el Proyecto I+D, del Ministerio de Ciencia y Tecnología, sobre «Las transformaciones del Derecho en la Sociedad de la Información y el Conocimiento», SEC2003-08529-C02-01/JUR.

UOC
www.uoc.edu