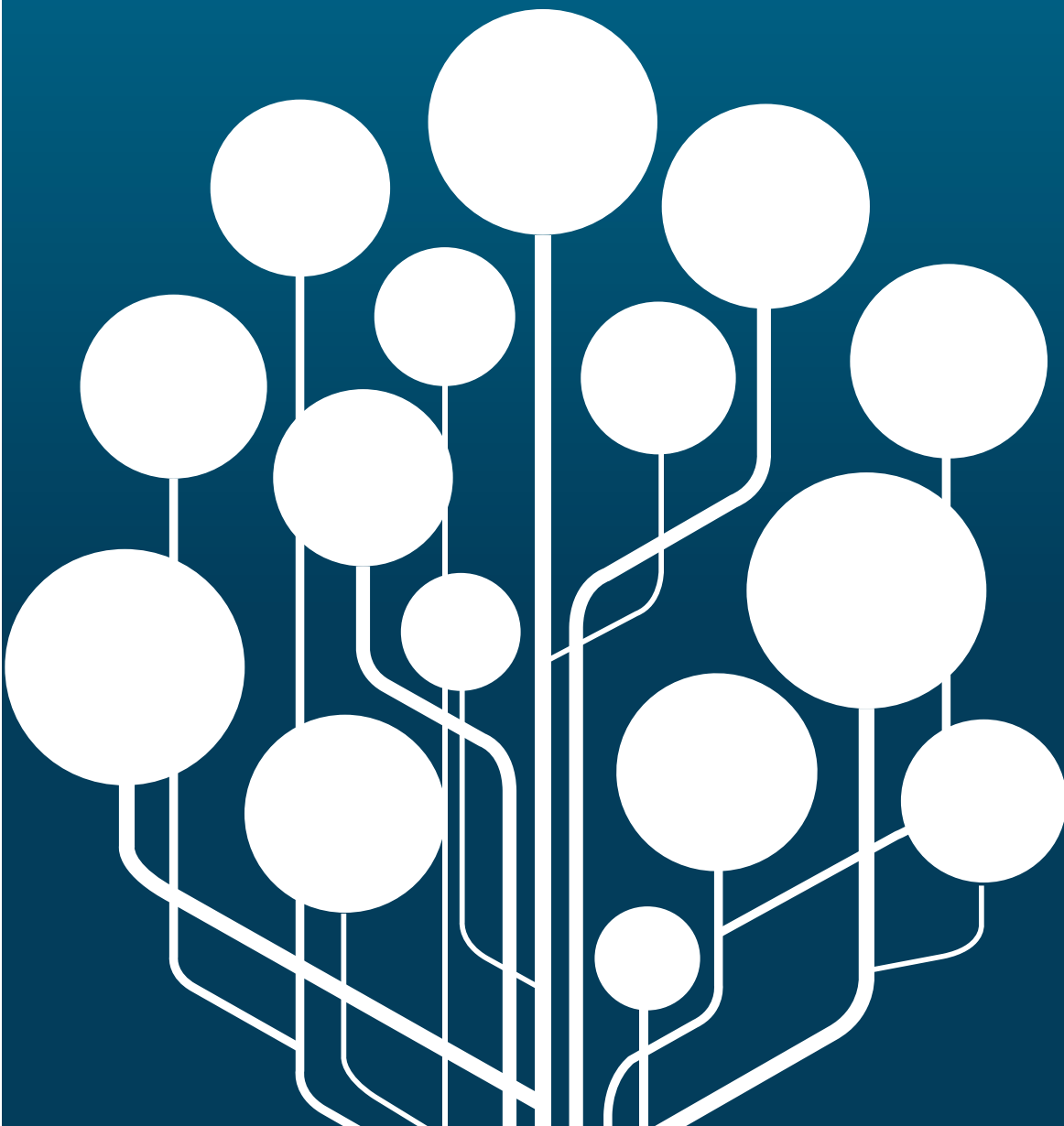


Retención de Datos Personales.
Invalidez de la Directiva 2006/24. Sentencia del TJUE.
Reforma de Telecomunicaciones 2014.
Reflexiones para México

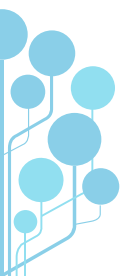


Retención de Datos Personales. Invalidez de la Directiva 2006/24. Sentencia del TJUE. Reforma de Telecomunicaciones 2014. Reflexiones para México

Héctor E. Guzmán Rodríguez¹

Entre abril y julio de 2014, ocurrieron dos hechos aparentemente inconexos. Por un lado, en Luxemburgo, el Tribunal de Justicia de la Unión Europea emitía una sentencia trascendental relativa a la protección de los derechos fundamentales sobre la vida privada y la protección de los datos personales, invalidando lo que se conoce como "Directiva de Retención de Datos". Por otro lado, en México fue publicada la nueva Ley Federal de Telecomunicaciones y Radiodifusión, que dentro de sus numerosas disposiciones introdujo obligaciones de conservación de datos de comunicaciones electrónicas que, en comparación, parecen reproducir algunas deficiencias que originaron la invalidez de la Directiva de referencia.

¹ Director del Área de Protección de Datos Personales y Privacidad de BGBG Abogados, consultor legal autónomo en materia de protección de datos personales en España.



El análisis de los antecedentes y de los razonamientos expresados por el Tribunal europeo podría aportar elementos importantes para valorar la constitucionalidad de las nuevas disposiciones legales que establecen la obligación de conservar datos sobre comunicaciones electrónicas, que la nueva normativa de telecomunicaciones ha introducido en nuestro país.

PALABRAS CLAVE: datos personales, privacidad, retención, reforma de telecomunicaciones, UE, México, Unión Europea, TJUE.



Introducción

En abril de 2014, el Tribunal de Justicia de la Unión Europea (TJUE) resolvió que la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, del 15 de marzo de 2006, 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 (la Directiva 2006/24), era inválida. Esto al considerar que en su adopción “el legislador de la Unión” había sobrepasado los límites que exige el respeto del “principio de proporcionalidad”. Esto en relación con los artículos 7, 8 y 52, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea, mediante medidas de injerencia desproporcionadas en los derechos a la privacidad y a la protección de datos personales.

La trascendencia de esta sentencia, en el ámbito europeo de los derechos fundamentales que se veían afectados, motivó reacciones de importantes grupos, tales como el Supervisor Europeo de Protección de Datos (SEPD)² y el Grupo de Trabajo de Protección de Datos del artículo 29 (GT29 o WP29),³ que en declaraciones individuales manifestaron:

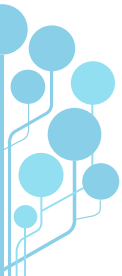
El SEPD acoge con satisfacción la sentencia del Tribunal de Justicia de la UE en el caso Digital Rights Ireland y Seitlinger y otros (asuntos acumulados C-293/12, C-594/12) sobre la invalidez de la Directiva sobre conservación de datos (Directiva 2006/24/CE). La misma sigue las consideraciones propuestas por el SEPD en el este procedimiento.

Consideramos esto como una sentencia histórica que limita la vigilancia gubernamental general sobre datos de comunicaciones (teléfono, textos, correo electrónico, acceso a Internet, etc.) permitida bajo dicha Directiva. Se destaca el valor asignado a la protección de los derechos fundamentales en el núcleo de la política de la UE en esta área crítica.

Estamos particularmente satisfechos de que el Tribunal de Justicia ha subrayado que la Directiva sobre conservación de datos constituye una grave e injustificada interferencia en el derecho fundamental a la privacidad consagrado en el artículo 7 de la Carta de los Derechos Fundamentales de la UE (European Data Protection Supervisor, 2014).

² El SEPD es una autoridad de supervisión independiente dedicada a la protección de los datos personales y la privacidad y la promoción de buenas prácticas en las instituciones y órganos de la UE.

³ El GT29 fue creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 24 de octubre de 1995. Se integra con representantes de las autoridades nacionales de protección de datos de la UE. Tiene carácter consultivo y actúa de forma independiente. Información oficial en: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.



Las autoridades europeas de protección de los datos, reunidos en el Grupo de Trabajo del artículo 29 (WP29), dan la bienvenida a la sentencia del Tribunal de Justicia de la Unión Europea (TJUE) que invalida la Directa de retención de datos. Instamos ahora a los Estados miembros de la UE, y a las instituciones competentes de la UE, a trazar las consecuencias de la resolución que establece un nuevo estándar para las legislaciones nacionales de retención de datos (Article 29 Data Protection Working Party, 2014).

No obstante lo anterior, y sólo tres meses después de la emisión de la sentencia de referencia, en México fue publicada la nueva Ley Federal de Telecomunicaciones y Radiodifusión (LFTR), que dio lugar a importantes reacciones⁴ en torno a las disposiciones establecidas en sus artículos 189 y 190, que prevén obligaciones para que los concesionarios de telecomunicaciones lleven a cabo la conservación de datos generados u obtenidos a partir de comunicaciones electrónicas efectuadas a través de cualquier tipo de línea, y su consulta y entrega en tiempo real a las “autoridades competentes”, a través de medios electrónicos.

En este sentido, frente a las disposiciones contenidas en los indicados artículos 189 y 190 de la LFTR y a la innegable influencia del derecho europeo en la normativa mexicana sobre protección de datos personales, resulta interesante conocer tanto el contenido y alcance de la Directiva 2006/24, como los razonamientos que llevaron al TJUE a declararla inválida, por considerar que la misma resulta contraria a los derechos de privacidad y de protección de datos personales.

4 Ver:

Reyes, J. J. (2014, 23 de julio). Piden al IFAI actuar contra ley telecom. El Economista. Recuperado de: <http://eleconomista.com.mx/sociedad/2014/07/23/piden-ifai-actuar-contra-ley-telecom>.

CNNExpansión (2014, 14 de julio). IFAI debe ir contra Ley Telecom: Fundar. CNNExpansión. Recuperado de: <http://www.cnnexpansion.com/economia/2014/07/14/ifai-debe-ir-contra-ley-telecom-fundar>.

Redacción AN (2014, 15 de agosto). #Documento: 219 organizaciones exigían al Ifai actuar contra ley telecom. Aristegui Noticias. Recuperado de: <http://aristeguinoticias.com/1508/mexico/organizaciones-pedian-al-ifai-interponer-accion-de-inconstitucionalidad-vs-ley-en-telecom/>.

La Unión Europea

La Unión Europea (UE) es una asociación económica y política singular, compuesta actualmente por 28 Estados miembros⁵ que se basa en el Estado de Derecho. Todas sus acciones se fundamentan en los Tratados⁶ que han sido aprobados y adoptados de forma voluntaria y democrática por todos sus Estados miembros. Una característica fundamental de la UE es la adopción de legislación supranacional que sus instituciones pueden aprobar y que los países miembros deben respetar.

Para el cumplimiento de sus objetivos, las instituciones de la UE adoptan diversos tipos de actos legislativos. Un Reglamento es un acto legislativo vinculante que debe aplicarse completamente en toda la UE y tiene efectos directos para todos los ciudadanos y residentes de los países miembros. En México, a pesar de su nombre, un Reglamento de la UE equivaldría a una Ley Federal. Por su parte, una Directiva es un acto legislativo en el que se establece un objetivo que todos los Estados miembros deben cumplir, pero que cada uno de ellos debe decidir, individualmente, cómo cumplir.

Los Estados miembros cumplen con los objetivos de las Directivas mediante de la transposición de sus disposiciones a su derecho nacional. En este sentido, mientras un país puede “adoptar” una Directiva a través de una Ley nacional, otros pueden hacerlo a través de reglamentos u otros instrumentos internos (Unión Europea, 2015⁷).

El Tribunal de Justicia de la Unión Europea (TJUE)⁸ es la autoridad judicial de la UE y tiene por misión garantizar “el respeto del Derecho en la interpretación y aplicación” de

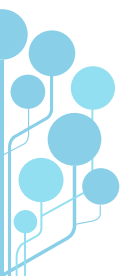
5 Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Países Bajos, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Polonia, Portugal, Reino Unido, República Checa, Rumanía, Suecia (Unión Europea, 2015).

6 Principales Tratados de la UE: Tratado de Lisboa; Tratado de Niza; Tratado de Ámsterdam; Tratado sobre la Unión Europea (Tratado de Maastricht); Acta Única Europea; Tratado de Fusión (Tratado de Bruselas); Tratados de Roma (Tratados CEE y EURATOM) y Tratado constitutivo de la Comunidad Europea del Carbón y del Acero (Unión Europea, 2015).

Cada Tratado vincula a los países miembros de la UE y en ellos se establecen los objetivos, las normas aplicables a sus instituciones, la forma y los procedimientos a través de los cuales se adoptan decisiones y la relación que existe entre la propia UE y sus Estados miembros.

7 Otros actos legislativos de la UE, irrelevantes a efectos de este estudio, son: las Decisiones, las Recomendaciones y los Dictámenes.

8 El TJUE (con sede en Luxemburgo) cuenta con un juez por cada país de la UE (28 actualmente) y está integrado por tres órganos jurisdiccionales: el Tribunal de Justicia, el Tribunal General, y el Tribunal de la Función Pública. El Tribunal de Justicia puede reunirse en Pleno, en Gran Sala (15 Jueces) o en Salas de cinco o tres Jueces. El TJUE se reúne en Gran Sala cuando así lo solicita un Estado Miembro o una institución que sea parte en el procedimiento y para los asuntos particularmente complejos o importantes.



los Tratados, además de interpretar el Derecho de la UE para garantizar que se aplique de la misma forma en todos los países miembros. Es en el marco de esta misión que el TJUE⁹:

- Controla la legalidad de los actos de las instituciones de la Unión Europea.
- Vela por que los Estados miembros respeten las obligaciones establecidas en los Tratados.
- Interpreta el Derecho de la Unión a solicitud de los jueces nacionales.

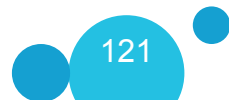
El origen del procedimiento seguido ante el TJUE, que concluyó con la invalidación de la Directiva 2006/24, lo constituyeron las cuestiones prejudiciales planteadas por el Tribunal Superior (High Court) de Irlanda y el Tribunal Constitucional de Austria (Verfassungsgerichtshof). Dado que los tribunales de cada país de la Unión Europea deben garantizar que el Derecho de ésta se aplique correctamente en cada uno de sus territorios, pero ante el riesgo de que cada uno de ellos interprete la legislación de manera divergente, se instituyó el procedimiento de las cuestiones prejudiciales, cuyo objeto último es el de garantizar la aplicación efectiva y homogénea de la legislación de la Unión.

En este sentido, los “jueces nacionales” pueden —y en ocasiones, deben— dirigirse al Tribunal de Justicia para pedir que éste precise una cuestión de interpretación del Derecho de la Unión, con el objeto de poder, por ejemplo, confirmar la correspondencia de una norma nacional con este Derecho. En ocasiones, la cuestión prejudicial puede tener por objeto el control de la validez de un acto del Derecho de la Unión, tal y como fue el caso en el procedimiento que declaró la invalidez de la “Directiva sobre retención de datos”. En la práctica, los jueces nacionales formulan las cuestiones prejudiciales en forma de preguntas, relacionadas con la compatibilidad de una disposición (nacional o europea) con el Derecho de la Unión¹⁰.

9 Disponible en el Tribunal de Justicia de la Unión Europea (sin fecha). Presentación general. Recuperado de: http://curia.europa.eu/jcms/jcms/Jo2_6999/.

10 Cabe señalar que a través de las cuestiones prejudiciales se han establecido algunos de los principios más importantes del Derecho de la Unión (antes llamado “Derecho Comunitario”), que en algunos casos iniciaron por cuestiones planteadas por órganos jurisdiccionales nacionales de primera instancia, instados por los propios litigantes de un asunto en concreto.

También es importante tener en cuenta que “el Tribunal de Justicia no responde mediante un mero dictamen, sino mediante una sentencia o un auto motivado. El órgano jurisdiccional nacional destinatario está vinculado por la interpretación efectuada a la hora de resolver el litigio que se le ha planteado. La sentencia del Tribunal de Justicia vincula asimismo al resto de los órganos jurisdiccionales nacionales que conozcan de un problema idéntico”.



Protección de datos personales en la UE

Si bien es cierto que actualmente la UE afronta un proceso de transformación en su marco legal de protección de datos personales¹¹, al día de hoy continúa vigente 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 datos¹² (la Directiva de Protección de Datos) de cuyos principios y disposiciones se nutrió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de nuestro país¹³.

La Directiva de referencia establece las disposiciones mínimas para amparar el derecho fundamental de protección de datos personales que cada uno de los Estados miembros de la UE han transpuesto en su normativa nacional y también es relevante en el marco de otras Directivas que referiremos en este estudio; a saber:

- (i) la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), y
- (ii) 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 (Directiva sobre la privacidad y las comunicaciones electrónicas).

Por otra parte, y tal y como ya hemos hecho referencia al inicio de este trabajo, en la UE existen entidades independientes que impulsan políticas de protección de datos, como el SEPD, o que, operando bajo las disposiciones de la Directiva de protección de datos, emiten informes interpretativos o documentos que sustentan posiciones de defensa de este derecho fundamental frente a las instituciones de la EU, como es el caso del GT29.

11 Ver Commission proposes a comprehensive reform of the data protection rules en el sitio web oficial de la Comisión Europea: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

12 Disponible en: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31995L0046>.

13 También es importante tomar en consideración, como fuente del derecho mexicano sobre protección de datos personales, la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, que en España constituye la normativa nacional a través de la cual se adoptaron las disposiciones de la Directiva de protección de datos.



La Directiva 2006/24. Objeto, ámbito y definiciones

Como acto legislativo dirigido a los Estados miembros, la “Directiva de retención de datos” establecía su objeto de la siguiente manera:

Artículo 1


Objeto y ámbito

1. La presente Directiva 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 o tratados por los mismos, para garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro.

Conforme a lo anterior, cada uno de los Estados miembros de la UE debían efectuar actos de transposición a su derecho nacional, basados en las reglas establecidas en la Directiva 2006/24 que, entre otras cuestiones, especificaba 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” que ellos mismos generan o que por cualquier otro motivo llegan a tratar.

En el inciso 2 de su artículo 1, la Directiva concreta su ámbito al establecer que sería aplicable a “los datos de tráfico y de localización” de personas físicas (y jurídicas) y los “datos relacionados” necesarios para identificar al abonado o al usuario registrado. Además, se establece expresamente que la misma no será aplicable al “contenido de las comunicaciones electrónicas”, que en todo caso incluye la “información consultada utilizando una red de comunicaciones electrónicas”. Así, por ejemplo, quedaban fuera del ámbito de la Directiva de retención de datos el contenido de los correos electrónicos o la información que una persona hubiese consultado por Internet durante una sesión.

Pero el objeto y el ámbito a que nos referimos no terminan de ser comprendidos si antes no echamos mano de determinadas definiciones que, en varios casos, no son aquellas contenidas en la propia Directiva invalidada, sino otras contenidas en: (i) la Directiva marco, y (ii) la Directiva sobre la privacidad y las comunicaciones electrónicas:



Red de comunicaciones electrónicas: los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluido Internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada.

Servicio de comunicaciones electrónicas: el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o ejerzan control editorial sobre ellos; [...];

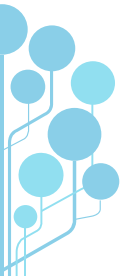
Red pública de comunicaciones: una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público;

«**Datos**»: los datos de tráfico y de localización y los datos relacionados necesarios para identificar al abonado o usuario;

«**Datos de tráfico**»: cualquier dato tratado a efectos de la conducción de una comunicación a través de una red de comunicaciones electrónicas o a efectos de la facturación de la misma;

«**Datos de localización**»: cualquier dato tratado en una red de comunicaciones electrónicas que indique la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público;

«**Comunicación**»: cualquier información intercambiada o conducida entre un número finito de interesados por medio de un servicio de comunicaciones electrónicas disponible para el público. No se incluye en la presente definición la información conducida, como parte de un servicio de radiodifusión al público, a través de una red de comunicaciones electrónicas, excepto en la medida en que la información pueda relacionarse con el abonado o usuario identificable que reciba la información;



«Correo electrónico»: todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la red o en el equipo terminal del receptor hasta que éste acceda al mismo.

«Usuario»: toda 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;

Abonado: cualquier persona física o jurídica que haya celebrado un contrato con un proveedor de servicios de comunicaciones electrónicas disponibles para el público para la prestación de dichos servicios;

«Servicio telefónico»: las llamadas (incluida la transmisión de voz, buzones vocales, conferencias y datos), los servicios suplementarios (incluido el reenvío o transferencia de llamadas) y los servicios de mensajería y servicios multimedia (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia);

«Identificador de usuario»: un identificador único asignado a las personas con motivo de su abono a un servicio de acceso a Internet o a un servicio de comunicaciones por Internet, o de su registro en uno de dichos servicios;

«Identificador de celda»: la identidad de la celda desde la que se origina o termina una llamada de teléfono móvil;

«Llamada telefónica infructuosa»: una comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación o en la que ha habido una intervención por parte del gestor de la red (Artículo 2 de Directiva Marco).

Amén de las anteriores definiciones, otras tantas contribuyen a comprender por qué el TJUE concluyó de forma clara y tajante que la Directiva exige, “conforme a su artículo 3 en relación con su artículo 5, apartado 1, la conservación de todos los datos de tráfico relativos a la telefonía fija, la telefonía móvil, el acceso a Internet, el correo electrónico por Internet y la telefonía por Internet. Por lo tanto, es aplicable a todos los medios de comunicación electrónica, cuyo uso está muy extendido y que tienen una importancia creciente en la vida cotidiana de las personas. Además, a tenor de su artículo 3, la Directiva comprende a todos los abonados y usuarios registrados. En consecuencia, constituye una injerencia en los derechos fundamentales de prácticamente toda la población europea” (TJUE, 2014).

Esta “afectación global” —entre otros elementos que a continuación habremos de referir—sería un elemento esencial en el análisis que el TJUE llevó a cabo, para concluir la desproporcionalidad de las medidas adoptadas por el legislador de la Unión, en el momento de adoptar la Directiva 2006/24.

La Directiva 2006/24. La obligación de conservar “datos”

La globalidad de la afectación a que nos referimos proviene de las “categorías de datos” que los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones debían conservar. Como veremos, se trata de un conjunto de información relacionada con prácticamente todos los aspectos de las comunicaciones electrónicas efectuadas por cualquier ciudadano, con excepción del contenido de las comunicaciones, que expresamente quedaba excluido del ámbito de la Directiva 2006/24.

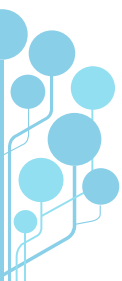
La obligación de conservación de datos —o de “retención de datos”, como se dio por denominarla de forma más o menos contundente— provenía de lo dispuesto por el artículo 3 de la Directiva analizada, que en lo que interesa dispone:

Artículo 3

Obligación de conservar datos

1. [...], los Estados miembros adoptarán medidas para garantizar que los datos especificados en el artículo 5 de la presente Directiva se conservan de conformidad con lo dispuesto en ella en la medida en que son generados o tratados por proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones que estén bajo su jurisdicción en el marco de la prestación de los servicios de comunicaciones de que se trate.
2. La obligación de conservar datos mencionada en el apartado 1 incluirá la conservación de los datos especificados en el artículo 5 en relación con las llamadas telefónicas infructuosas [...].

Además, y acorde con su objeto —fines de investigación, detección y enjuiciamiento de delitos graves, tal como se definen en la legislación nacional de cada Estado miembro—, en el artículo 4 se disponía la obligación de los Estados miembros de adoptar medidas



que garantizaran que los datos conservados solamente serían proporcionados a las autoridades nacionales competentes, en casos específicos y de conformidad con la legislación nacional de cada uno de ellos.

Dicho todo lo cual, resulta ya indispensable conocer cuáles son las “categorías de datos” que los proveedores de servicios de comunicaciones electrónicas debían conservar conforme a la Directiva 2006/24(artículo 5):

- a) datos necesarios para rastrear e identificar el origen de una comunicación;
- b) datos necesarios para identificar el destino de una comunicación;
- c) datos necesarios para identificar la fecha, hora y duración de una comunicación;
- d) datos necesarios para identificar el tipo de comunicación;
- e) datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación, y
- f) datos necesarios para identificar la localización del equipo de comunicación móvil.

Esta lista, al parecer lo suficientemente larga, en realidad no está completa, pues cada una de las categorías anteriores estaba integrada por los siguientes tipos de datos:


a) Datos necesarios para rastrear e identificar el origen de una comunicación

1) con respecto a la telefonía de red fija y a la telefonía móvil:

i) el número de teléfono de llamada,

ii) el nombre y la dirección del abonado o usuario registrado;

2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

- 
- i) la identificación de usuario asignada,
 - ii) la identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía,
 - iii) el nombre y la dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo Internet (IP), una identificación de usuario o un número de teléfono;

b) Datos necesarios para identificar el destino de una comunicación

1) con respecto a la telefonía de red fija y a la telefonía móvil:

- i) el número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas,
- ii) los nombres y las direcciones de los abonados o usuarios registrados;

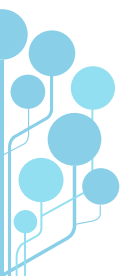
2) con respecto al correo electrónico por Internet y a la telefonía por Internet:

- i) la identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet,
- ii) los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación;

c) Datos necesarios para identificar la fecha, hora y duración de una comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil:

la fecha y hora del comienzo y fin de la comunicación,



2) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) la fecha y hora de la conexión y desconexión del servicio de acceso a Internet, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, así como la identificación de usuario del abonado o del usuario registrado,

ii) la fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario;

d) Datos necesarios para identificar el tipo de comunicación:

1) con respecto a la telefonía de red fija y a la telefonía móvil:

el servicio telefónico utilizado,

2) con respecto al correo electrónico por Internet y a la telefonía por Internet:

el servicio de internet utilizado;

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

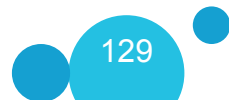
1) con respecto a la telefonía de red fija:

los número de origen y destino,

2) con respecto a la telefonía móvil:

i) los números de teléfono de origen y destino,

ii) la identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada,



iii) la identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada,

iv) la IMSI de la parte que recibe la llamada,

v) la IMEI de la parte que recibe la llamada,

vi) en el caso de los servicios anónimos de pago por adelantado, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio;

3) con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) el número de teléfono de origen en caso de acceso mediante marcado de números,

ii) la línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación;

f) datos necesarios para identificar la localización del equipo de comunicación móvil:

1) la etiqueta de localización (identificador de celda) al comienzo de la comunicación,

2) los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

Como "refuerzo" a lo ya establecido en el apartado 2 del artículo 1, el artículo 5 de la Directiva 2006/24 concluía reiterando que "no podrá conservarse ningún dato que revele el contenido de la comunicación".



Otras disposiciones de la Directiva 2006/24

Aspectos que también resultan destacables de este ordenamiento europeo, y que también fueron tomados en cuenta por el TJUE al emitir su Sentencia, son las disposiciones relativas a los períodos de conservación de los datos, a los principios de seguridad de los mismos y a los requisitos de almacenamiento para los datos conservados. En cuanto al primero, el artículo 6 de la Directiva 2006/24 disponía que “los Estados miembros garantizarán que las categorías de datos mencionadas en el artículo 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.”

Por lo que se refiere a los principios de seguridad de los datos que debían conservarse (artículo 7), estos pueden resumirse de la siguiente forma:

- Serán de la misma calidad y estarán sometidos a las mismas normas de seguridad y protección que los datos existentes en la red;
- Estarán sujetos a las medidas técnicas y organizativas adecuadas para protegerlos de la destrucción accidental o ilícita, pérdida accidental o alteración, así como almacenamiento, tratamiento, acceso o divulgación no autorizados o ilícitos;
- Estarán sujetos a medidas técnicas y organizativas apropiadas para velar porque sólo puedan acceder a ellos las personas especialmente autorizadas,
- Los datos, excepto los que hayan sido accesibles y se hayan conservado, se destruirán al término del período de conservación.

Los requisitos de almacenamiento previstos por la Directiva (artículo 8) se referían a la garantía que debían ofrecer los Estados miembros para que los datos especificados en el artículo 5 se guardaran “de manera que los datos conservados y cualquier otra información necesaria con ellos relacionada puedan transmitirse sin demora cuando las autoridades competentes así lo soliciten”.

Identificación de la sentencia que invalidó la Directiva 2006/24. Cuestiones prejudiciales y derechos fundamentales ponderados

La identificación formal de la sentencia que analizamos, tal y como ha sido publicada¹⁴, puede resumirse en los siguientes elementos:

SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 8 de abril de 2014

«Comunicaciones electrónicas — Directiva 2006/24/CE — Servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones — Conservación de datos generados o tratados en relación con la prestación de tales servicios — Validez — Artículos 7, 8 y 11 de la Carta de los Derechos Fundamentales de la Unión Europea»

En los asuntos acumulados C-293/12 y C-594/12, que tienen por objeto sendas peticiones de decisión prejudicial planteadas, con arreglo al artículo 267 TFUE, por la High Court (Irlanda) y el Verfassungsgerichtshof (Austria),

Dentro de las diversas cuestiones prejudiciales planteadas ante el TJUE, las siguientes tienen una relevancia especial en relación con el fallo que declaró la invalidez de la Directiva 2006/24.

Por parte de la High Court de Irlanda:

¿Es compatible la Directiva 2006/24 con el derecho al respeto de la vida privada establecido en el artículo 7 de la [Carta de los Derechos Fundamentales de la Unión Europea; en lo sucesivo, «Carta»] [...]?

¿Es compatible la Directiva 2006/24 con el derecho a la protección de los datos de carácter personal establecido en el artículo 8 de la Carta?

Por el Verfassungsgerichtshof de Austria:

Respecto de la validez de actos adoptados por los órganos de la Unión:

¹⁴ Recuperada el 20 de enero de 2015 mediante búsqueda en N° de Asunto "C-293/12", en http://curia.europa.eu/jcms/jcms/j_6/.



¿Son los artículos 3 a 9 de la Directiva 2006/24 compatibles con los artículos 7, 8 y 11 de la [Carta]?

En este sentido, para iniciar el conocimiento de los razonamientos esgrimidos a lo largo de la sentencia que se analiza, el conocimiento de los artículos 7 y 8 de la Carta resulta elemental:

Artículo 7. Respeto de la vida privada y familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Artículo 8. Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Además, y debido a que la Directiva 2006/24 contiene disposiciones que limitan el ejercicio de derechos reconocidos por la Carta, es necesario conocer de qué forma el mismo ordenamiento prevé la posible limitación de dichos derechos:

Artículo 52

Alcance de los derechos garantizados

1. Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

Consideraciones de la Sentencia. Sobre la pertinencia de los artículos 7 y 8 de la Carta

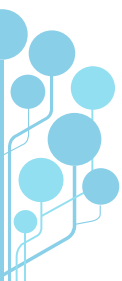
Llegados a este punto, debemos abordar la manera en que el TJUE llevó a cabo el análisis sobre la validez de la Directiva 2006/24, es decir, el análisis sobre la cabida de dicho ordenamiento en el conjunto de disposiciones que protegen los derechos y libertades establecidos por el derecho de la Unión. Este órgano jurisdiccional determinó que, la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, de conservar los datos enumerados en el artículo 5 de dicha Directiva, para que las autoridades nacionales competentes puedan acceder a ellos, "suscita cuestiones relativas a la protección de la vida privada y de las comunicaciones reconocida en el artículo 7 de la Carta [y] a la protección de los datos de carácter personal establecida en el artículo 8 de ésta [...]" (TJUE, 2014).

Se colige que los datos cuya conservación se establece como obligatoria permiten, en particular, "saber con qué persona se ha comunicado un abonado o un usuario registrado y de qué modo, así como determinar el momento de la comunicación y el lugar desde la que ésta se ha producido. Además, permiten conocer la frecuencia de las comunicaciones del abonado o del usuario registrado con determinadas personas durante un período concreto" (TJUE, 2014).

Y en esta línea de razonamiento, el TJUE apunta que los datos que deben conservarse, considerados en su conjunto, "pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan" (TJUE, 2014).

Sin lugar a dudas, el TJUE efectúa una aproximación realista de la información que es posible obtener a partir del conjunto de datos que se ordenan conservar a los prestadores de servicios de comunicaciones electrónicas, entendida como hábitos de la vida cotidiana, su lugar de residencia o trabajo, las personas con las cuales se relaciona, los lugares a los cuales se desplaza. Un conjunto de datos que, a final de cuentas, permite generar un perfil de todos los ciudadanos que utilizan medios electrónicos para comunicarse, relacionado evidentemente con su vida privada.

Es por ello que en su análisis el juzgador europeo afirma de forma concreta que: "La conservación de datos para su eventual acceso por las autoridades nacionales competentes, según se establece en la Directiva 2006/24, afecta de manera directa y específica a la vida privada y, por tanto, a los derechos que garantiza el artículo 7 de



la Carta. Además, el artículo 8 de la Carta también es aplicable a dicha conservación de datos, puesto que constituye un tratamiento de datos de carácter personal en el sentido de ese artículo y debe, por tanto, cumplir necesariamente los requisitos de protección de datos que se derivan de dicho artículo [...]” (TJUE, 2014).


Estas conclusiones permiten avanzar al siguiente punto del razonamiento efectuado por el TJUE, ya que no cabe duda de que la validez de la Directiva 2006/24 debe examinarse “a luz de los artículos 7 y 8 de la Carta”(TJUE, 2014), pues resulta claro que nos encontramos frente a un ordenamiento cuyo cumplimiento, a cargo de los sujetos obligados y de las “autoridades” que pueden tener acceso a los datos conservados, genera una afectación en la vida privada de las personas y en su derecho fundamental a la protección de sus datos personales.

Consideraciones de la Sentencia. Sobre la existencia de una injerencia en los derechos reconocidos por los artículos 7 y 8 de la Carta

La cuestión relativa a la existencia de una injerencia en los derechos fundamentales previstos en los artículos de referencia, la aborda el TJUE de forma directa al razonar que, la obligación de conservación de los datos previstos en el artículo 5, apartado 1, de la Directiva, y el acceso que se concede a las autoridades nacionales competentes a estos, constituye “una excepción al régimen de protección del derecho de respeto a la vida privada [...], con respecto al tratamiento de los datos de carácter personal en el sector de las comunicaciones electrónicas” (TJUE, 2014).

Cabe señalar que en este punto la sentencia clarifica y recuerda que: “para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada, carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia [...]” (TJUE, 2014). Esta aclaración resulta esencial en cualquier tipo de análisis que pueda efectuarse sobre la existencia o inexistencia de una injerencia en el derecho a la privacidad, derivado de una norma que determine la obligación de conservar datos como los que hemos identificado.

Después de todo, es verdad que el tipo de datos que deban conservarse (sensibles, patrimoniales, o identificativos, por ejemplo) o la existencia de una “molestia” (inconveniente) en la vida cotidiana de los interesados, no constituyen elementos



diferenciadores o excluyentes que permitan concluir que dicha injerencia no existe. En otras palabras, el hecho de que una entidad, por mandato legal, deba conservar este tipo de datos, y el hecho de que una autoridad, por habilitación igualmente legal, pueda acceder a dichos datos, constituyen en sí mismos actos de injerencia en este derecho fundamental¹⁵.

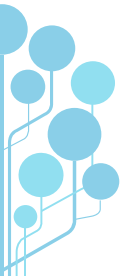
En cuanto a la existencia de una injerencia en el derecho fundamental a la protección de datos personales (datos de carácter personal), el TJUE resuelve la cuestión en tres líneas, pues resulta obvio que la Directiva 2006/24 “establece un tratamiento de datos de carácter personal” (TJUE, 2014) identificable, precisamente como la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de una red pública de comunicaciones, de conservar los datos que ya hemos identificado.

En este punto, es importante recordar que, la Directiva de protección de datos define como “tratamiento de datos personales”: cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción (Directiva de protección de datos, artículo 2.b). Una definición que sirvió de referencia a la propia que contiene nuestra Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPD, artículo 3, fracción XVIII).

Conforme a lo anterior, no es óbice para concluir que existe una injerencia en el derecho fundamental a la protección de datos personales el hecho de que la conservación de datos de comunicaciones electrónicas venga impuesta por un ordenamiento y que no obedezca dicha conservación a la voluntad de las entidades que los generan. El tratamiento de datos personales puede derivar de finalidades legítimas y propias de aquellos responsables que desean o deben tratarlos, o ser la consecuencia del cumplimiento de disposiciones legales que prevén y exigen —como en el caso concreto— llevar a cabo dicho tratamiento, pero en todos los casos nos encontramos con un tratamiento de datos personales.

Finalmente, y como corolario a esta parte de su razonamiento, en la sentencia analizada el TJUE concluye que la injerencia que supone la Directiva 2006/24 en los derechos fundamentales que se reconocen en los artículos 7 y 8 de la Carta resulta “de gran magnitud y debe considerarse especialmente grave”.

15 Ver, TJUE, 2014, apartados 34 y 35.



Consideraciones de la sentencia. ¿Está justificada la injerencia en los derechos garantizados por los artículos 7 y 8 de la Carta?

Llegados a este punto, existen elementos para afirmar que la existencia de una injerencia en los derechos a la vida privada y a la protección de datos personales ha quedado corroborada; pero es necesario aclarar que lo anterior no constituye, por sí mismo, base suficiente para considerar que un ordenamiento, como la Directiva 2006/24, es contrario al derecho de la UE. Como hemos indicado previamente, en la propia Carta se prevé la posibilidad de que los derechos y libertades que ésta protege puedan verse limitados. El apartado 1 de su artículo 52 establece que cualquier limitación deberá:

- Ser establecida por la ley,
- Respetar el contenido esencial de dichos derechos y libertades,
- Respetar el principio de proporcionalidad,
- Ser necesaria,
- Responder efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás.

Al abordar el análisis de estos requisitos, el juzgador europeo arriba a conclusiones que pudieran parecer suficientes para sustentar la validez y el encaje de la Directiva en el derecho de la UE, pero veremos dentro de poco que éstas no resultaron suficientes para sostener la validez de aquélla. En primer lugar, el TJUE concluye que si bien es cierto que la conservación de datos que impone la Directiva 2006/24 constituye una injerencia especialmente grave en los derechos reconocidos en el artículo 7 de la Carta, no puede considerarse que vulnere el contenido esencial de los mismos, dado que el apartado 2 del artículo 1 de aquélla prevé que su implementación por los Estados miembros no debe permitir conocer el contenido de las comunicaciones, como tal.

También indica que la Directiva tampoco vulnera el contenido esencial del derecho fundamental a la protección de los datos de carácter personal ya que el artículo 7 establece una regla según la cual los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de telecomunicaciones deben respetar determinados principios de protección y de seguridad de los datos. Y, con arreglo a dichos principios, “los Estados miembros velarán por que se adopten medidas técnicas y organizativas adecuadas contra la destrucción accidental o ilícita de los datos y su pérdida o alteración accidental” (TJUE, apartado 40, 2014).



Adicionalmente, la sentencia también concluye que las disposiciones de la Directiva 2006/24 sí responden a un objetivo de interés general, puesto que el objetivo principal de la misma es el de “contribuir a la lucha contra la delincuencia grave y, en definitiva, a la seguridad pública” (TJUE, apartado 41, 2014). Y en este sentido, valiéndose de la jurisprudencia del propio TJUE, recuerda que “la lucha contra el terrorismo internacional para el mantenimiento de la paz y la seguridad internacionales es un objetivo de interés general de la Unión”. Lo mismo ocurre en lo que respecta a “la lucha contra la delincuencia grave para garantizar la seguridad pública” (TJUE, apartado 42, 2014).

Además, el TJUE no pasa por alto que el artículo 6 de la Carta no sólo establece el derecho de toda persona a la libertad, sino también a la seguridad. En definitiva, el TJUE reconoce que la conservación de los datos “para su eventual acceso por parte de las autoridades nacionales competentes [...] responde efectivamente a un objetivo de interés nacional” (TJUE, apartado 44, 2014). No cabe duda, pues, que existen objetivos de interés general que sustentan la necesidad de un ordenamiento que regule y permita la conservación de datos de comunicaciones electrónicas y su acceso para finalidades de prevención de delitos graves, incluso (o precisamente) enfrentados con los derechos fundamentales en juego.

En este sentido, consideramos fundamental dejar claro que dentro del objeto de este estudio, la necesidad de la medida en cuestión no es materia de debate si la misma es definida de forma clara y precisa. El “crecimiento significativo de las posibilidades de las comunicaciones electrónicas” y el valor de los datos de las comunicaciones como “una herramienta valiosa en la prevención de delitos y la lucha contra la delincuencia, en especial la delincuencia organizada” (TJUE, apartado 43, 2014) es incuestionable y existen pocos argumentos en contra de dicha importancia y utilidad.

Sin embargo, es indispensable que la existencia del interés general que puede justificar la injerencia en determinados aspectos de la vida privada, no ensombrezcan ni disminuya la otra cara de la moneda: la forma y el alcance de la medida no puede exceder de lo estrictamente necesario para alcanzar sus fines, pues son precisamente derechos fundamentales los que están en juego.

Dicho lo anterior, y recordando que tenemos frente a nosotros una injerencia constatada, podría decirse que “hasta ahora todo bien”. Sin embargo, queda un requisito por salvar: la proporcionalidad de dicha injerencia.





Del principio de proporcionalidad

Según recuerda la propia sentencia, la jurisprudencia del TJUE establece que “el principio de proporcionalidad exige que los actos de las instituciones de la Unión sean adecuados para lograr los objetivos legítimos perseguidos por la normativa de que se trate y no rebasen los límites de lo que resulta apropiado y necesario para el logro de dichos objetivos” (TJUE, apartado 46, 2014). En esta línea de razonamiento se reconoce, en primer lugar, que la conservación de datos impuesta por la Directiva “puede considerarse adecuada para lograr el objetivo perseguido” (TJUE, apartado 49, 2014) pero además debe atenderse a la necesidad de la medida.

Es en este punto en que el TJUE comienza a exponer las “debilidades” de la Directiva indicando, en primer lugar, que el objetivo de interés general que le ha sido reconocido no puede por sí solo justificar que una medida de conservación, tal y como ha sido establecida por este ordenamiento, se considere necesaria a los efectos de la lucha contra la delincuencia grave y el terrorismo. Y es que, tal y como recalca el Tribunal, la protección de los datos personales tiene una importancia especial para el derecho al respeto a la vida privada que consagra el artículo 7 de la Carta (TJUE, apartado 53, 2014); recordando además que las excepciones a la protección de los datos personales y las restricciones a la protección del derecho a la intimidad, deben establecerse “sin sobrepasar los límites de lo estrictamente necesario” (TJUE, apartado 52, 2014). Es dentro de esta línea de razonamiento que el TJUE define (TJUE, apartado 54, 2014) ciertos requisitos que, desde nuestro punto de vista, debemos tener en cuenta en el momento de analizar una normativa como lo que se analiza, que claramente establece medidas de excepción o restricción a la protección de los derechos fundamentales a la vida privada y la protección de datos personales. Dicha normativa:

- Debe establecer reglas clara y precisas que regulen el alcance y la aplicación de la medida en cuestión (la retención de datos y su comunicación a terceros).
- Debe establecer exigencias mínimas, de forma tal que las personas cuyos datos deban conservarse dispongan de garantías suficientes que aseguren la protección eficaz de sus datos personales, contra riesgos de abuso (uso inadecuado, por ejemplo) y contra cualquier acceso ilícito.

Y es que, como recuerda el Tribunal, la necesidad de disponer de tales garantías “es especialmente importante cuando [...] los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a dichos datos” (TJUE, apartado 55, 2014), pues es obvio que tales datos serían resguardados en medios automatizados de los responsables, que pueden verse expuestos a ataques informáticos o, simplemente, a una inadecuada regulación interna sobre aquellos perfiles de personas que pueden tener acceso a los datos conservados. Tampoco se garantiza, como el propio TJUE apuntaría, que los datos serían tratados únicamente en territorio “nacional”.

Entonces, ¿la injerencia que supone la Directiva 2006/24 se limita a lo estrictamente necesario?

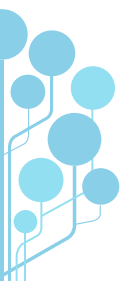
A partir de este momento y con base en la pregunta anterior comenzaremos a encontrar los razonamientos que sirvieron de base para declarar la invalidez de la Directiva. Para hacerlo, el juzgador europeo recuerda que dicho ordenamiento (TJUE, apartado 56 y 57, 2014):

- es aplicable a todos los medios de comunicación electrónica,
- comprende a todos los abonados y usuarios registrados,
- barca de manera generalizada a todas las personas, medios de comunicación electrónica y datos relativos al tráfico, y
- no establece ninguna diferenciación, limitación o excepción en función de su objetivo.

Lo cual, tras una lectura pormenorizada de la Directiva, resulta evidente, puesto que ésta afecta de manera global “a todas las personas que utilizan servicios de comunicaciones electrónicas, sin que las personas cuyos datos se conservan se encuentren, ni siquiera indirectamente, en una situación que pueda dar lugar a acciones penales” (TJUE, apartado 58, 2014)

Es decir, que las disposiciones de esta normativa aplican, sin distinciones, incluso a ciudadanos respecto de los cuales ni siquiera existen indicios directos o indirectos de haber participado en la comisión de delitos graves. Los datos, de todos por igual, conservados para perseguir delitos graves, aunque la mayoría de ellos no tenga la mínima relación con conductas delictivas. Sin duda, estamos frente a medidas desproporcionadas en relación con el objetivo perseguido. A mayor abundamiento, podemos ver que la Directiva invalidada, a pesar de responder a un objetivo de interés nacional, “no exige ninguna relación entre los datos cuya conservación se establece y una amenaza para la seguridad pública” (TJUE, apartado 59, 2014), ni establece límites perfectamente alcanzables, como datos referentes a:

- un período temporal,
- una zona geográfica determinada,
- un círculo de personas concretas que puedan estar implicadas de una manera u otra en un delito grave, o
- personas que por otros motivos podrían contribuir, mediante la conservación de sus datos, a la prevención, detección o enjuiciamiento de delitos graves (TJUE, apartado 59, 2014).



Por si lo anterior no fuera suficiente, se subraya que la Directiva (TJUE, apartado 61, 2014) no precisa las condiciones materiales y de procedimiento relacionadas con el acceso de las autoridades nacionales competentes a los datos y su utilización posterior. Y es que, el artículo 4 del ordenamiento puesto a revisión, “no dispone expresamente que el acceso y la utilización posterior de los datos de que se trata deberán limitarse estrictamente a fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos” (TJUE, apartado 62, 2014).

Además, nos encontramos con que la Directiva:

- no establece ningún criterio objetivo que permita limitar el número de personas que disponen de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario, teniendo en cuenta el objetivo perseguido;
- ni supedita el acceso a los datos conservados, a un control previo efectuado, bien por un órgano jurisdiccional, bien por un organismo administrativo autónomo, cuya decisión tenga por objeto limitar el acceso a los datos y su utilización a lo estrictamente necesario para alcanzar el objetivo perseguido.

Desde luego, es previsible que existan puntos de vista que indiquen que estos “detalles” pueden ser definidos y desarrollados a través de normativa reglamentaria (como es el caso de México), posición que encuentro difícil de compartir, dado que las condiciones y procedimientos de limitación y restricción de derechos fundamentales no puede quedar como un aspecto secundario, a cargo de una normativa subsidiaria. Como punto final de su análisis, el TJUE resalta que, por lo que se refiere al periodo de conservación de los datos, no se establece ninguna distinción entre las categorías de datos a que se refiere el artículo 5 de la Directiva, en función de su posible utilidad para el objetivo perseguido o de las personas afectadas (TJUE, apartado 63, 2014). Se establece pues, sin distinciones de ningún tipo, un período genérico de conservación.

Tras todas estas consideraciones, el TJUE no duda en afirmar que la Directiva 2006/24 (TJUE, apartado 65 a 68, 2014):

- no establece reglas claras y precisas que regulen el alcance de la intrusión en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta;
- constituye una injerencia en los derechos fundamentales de gran magnitud y especial gravedad en el ordenamiento jurídico de la Unión, sin que esta injerencia esté regulada de manera precisa por disposiciones que permitan garantizar que se limita efectivamente a lo estrictamente necesario;



- no contiene garantías suficientes que permitan asegurar una protección eficaz de los datos conservados contra los riesgos de abuso y contra cualquier acceso y utilización ilícitos respecto de tales datos, toda vez que:
- No establece reglas específicas y adaptadas a la gran cantidad de datos cuya conservación, al carácter sensible de estos datos y al riesgo de acceso ilícito a ellos.
- No garantiza que los proveedores apliquen un nivel especialmente elevado de protección y seguridad a través de medidas técnicas y organizativas.
- No garantiza la destrucción definitiva de los datos al término de su periodo de conservación.
- No obliga a que los datos en cuestión se conserven en el territorio de la UE.

Por lo que concluye que, "al adoptar la Directiva 2006/24, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los artículos 7, 8 y 52, apartado 1, de la Carta" (TJUE, apartado 69, 2014). Y, conforme a todo lo anterior, la Gran Sala del Tribunal de Justicia del TJUE, declaró:

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 de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, es inválida.

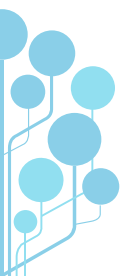
Escenario en México

Sobre el derecho al respeto de la vida privada y a la protección de datos personales, en nuestra Constitución y la legislación federal

El texto vigente de nuestra Carta Magna presenta las siguientes características:

- No menciona, ni una sola vez, los conceptos "privacidad" ni "intimidad".
- El concepto "vida privada" aparece dos veces en el artículo 6:

Artículo 6. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, [...].



A. Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se registrarán por los siguientes principios y bases: [...]

II. La información que se refiere a la **vida privada** y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

- Mediante diversas tesis,¹⁶ la Suprema Corte de Justicia de la Nación ha identificado que la “garantía de privacidad” está contenida en el artículo 16 de la Carta Magna.
- El mismo artículo 16 constitucional prevé, después de la reforma publicada en el *Diario Oficial de la Federación*, el derecho a la protección de los datos personales, en los siguientes términos:

Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

16 Ver por ejemplo:

- SECRETO BANCARIO. EL ARTÍCULO 117 DE LA LEY DE INSTITUCIONES DE CRÉDITO NO VIOLA LA GARANTÍA DE PRIVACIDAD. Tesis 1a. CXLI/2011, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXXIV, Julio de 2011, p. 310.
- DERECHO A LA INVOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA COMUNICACIÓN. Tesis 1a. CLV/2011, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXXIV, Agosto de 2011, p. 221.
- DERECHO A LA PRIVACIDAD O INTIMIDAD. ESTÁ PROTEGIDO POR EL ARTÍCULO 16, PRIMER PÁRRAFO, DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Tesis 2a. LXIII/2008, Semanario Judicial de la Federación y su Gaceta, Novena Época, t. XXVII, Mayo de 2008, p. 229.

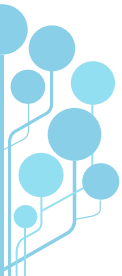
- Finalmente, cabe mencionar que el mismo numeral 16 contiene otros dos conceptos relevantes en el marco de este estudio: “comunicaciones privadas” y “privacía”:

Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas. El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley.

Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.

Por otro lado, la legislación federal sobre protección de datos personales (en posesión de los particulares) ha tenido un desarrollo significativo desde que la protección de este tipo de información fue incluida como derecho fundamental en nuestra Carta Magna¹⁷. Cuestión la anterior que, por sí misma y con independencia de la existencia de un organismo autónomo como el Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI), no es suficiente para garantizar que en nuestro ordenamiento jurídico no puedan ser aprobadas, publicadas y entrar en vigor disposiciones que vulneren, tanto este derecho fundamental, como el derecho a la privacidad, tal y como aparece que vulneran las disposiciones de los artículos 189 y 190 de la LFTR.

17 Al día de hoy, además de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPD), han sido publicados: el Reglamento de la LFPD; los Lineamientos del Aviso de Privacidad; las Recomendaciones en Materia de Seguridad de Datos Personales; los Parámetros de Autorregulación en materia de Protección de Datos Personales; el Acuerdo del Pleno del IFAI, por el que se aprueba el Proyecto de Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante y se instruye su publicación oficial; además de diversas publicaciones sobre el derecho a la protección de datos personales y recomendaciones a los Responsables para el cumplimiento de la LFPD.



Pues es de considerar que las disposiciones contenidas en los artículos de referencia adolecen de gran parte de las mismas deficiencias que fueron señaladas por el TJUE en la sentencia que hemos intentado resumir, ya que en su conjunto permiten advertir:

- Que no se garantiza que los datos únicamente serán utilizados para prevenir y sancionar delitos, ni qué tipo de delitos se busca prevenir y sancionar con apoyo en el acceso a los datos de comunicaciones que se enumeran (de forma genérica) en la fracción II del artículo 190 de la LFTR. De hecho, el marco establecido por los artículos 189 y 190 parece dejar la puerta abierta para que los datos retenidos puedan ser usados para la investigación de infracciones administrativas.
- Que, como resultado de lo anterior, no se limitan los datos que deben ser retenidos por los concesionarios a: un período temporal de investigación, una zona geográfica determinada en el marco de una investigación, un número o grupo de personas concretas que pudieran estar implicadas en conductas tipificadas como delitos (graves), otros tipos de personas que pudieran contribuir, a través de la retención de sus datos, a la prevención, persecución y enjuiciamiento de delitos.

En suma, nuestro ordenamiento vigente ordena la conservación de los datos de comunicaciones electrónicas, de cualquier persona que utilice redes de comunicaciones, sin ningún tipo de distinción entre los usuarios o abonados de los servicios correspondientes, una injerencia global e indiscriminada.

- Que en este ordenamiento federal no existen reglas clara y precisas que regulen y limiten el alcance de la injerencia que la retención de datos de comunicaciones establece a cargo de los concesionarios de telecomunicaciones y, además, de “autorizados y proveedores de servicios de aplicaciones y contenidos”; estos últimos, no definidos en la LFTR.
- Que no existen límites que garanticen, a favor de los gobernados, que el tratamiento de los datos retenidos se limitará a lo estrictamente necesario, más allá de la declaración, carente de tipificación adecuada, que indica:

Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.

- Que no se han establecido obligaciones específicas sobre las medidas de seguridad que los obligados a la retención de estos datos deben adoptar para garantizar que estos serán tratados por personas no autorizadas, limitándose a ordenar que éstas deberán ser “medidas técnicas necesarias respecto de los datos objeto de conservación”.

- Que no se garantiza ni ordena que los datos retenidos no puedan ser tratados fuera del territorio de los Estados Unidos Mexicanos dejando abierta la posibilidad real de que su conservación pueda ser encomendada a terceros ubicados fuera de nuestro territorio nacional.

En suma, creemos que es posible considerar que en nuestro ordenamiento jurídico ha encontrado cabida una Ley Federal que contiene disposiciones que representan una injerencia grave en los derechos fundamentales a la vida privada y a la protección de datos personales que, sin haber definido claramente los intereses generales que con su adopción se persiguen, contiene disposiciones que no se limitan a lo estrictamente necesario para que las “autoridades competentes” puedan cumplir con finalidades específicas, excediendo límites que respeten el contenido esencial de dichos derechos fundamentales.

Finalmente, no quisiera concluir este análisis sin dejar de mencionar que nuestra Suprema Corte de Justicia, de forma aislada al día de hoy, ya ha tenido oportunidad de pronunciarse respecto a la protección que nuestra Constitución brinda a los “datos de tráfico de comunicaciones”. Ha indicado, en línea con los razonamientos que hemos analizado del TJUE, que dichos datos “en muchas ocasiones ofrecen información sobre las circunstancias en que se ha producido la comunicación, afectando así, de modo directo o indirecto, la privacidad de los comunicantes”¹⁸.

Esto sin duda permite anticipar que nuestros Ministros son sensibles también al alcance y naturaleza de la injerencia que la conservación de datos de comunicaciones electrónicas puede tener sobre los derechos a la privacidad y a la protección de datos personales de cualquier ciudadano. Quedaría por resolver si estas consideraciones, en el marco de las difusas finalidades contenidas en los artículos 189 y 190 de la LFTR, serían igualmente defendidas en un hipotético análisis de constitucionalidad al que dichas disposiciones deberían ser sometidas.

18 SCJN. (2011, agosto). DERECHO A LA INVOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU OBJETO DE PROTECCIÓN INCLUYE LOS DATOS QUE IDENTIFICAN LA COMUNICACIÓN. Tesis 1a. CLV/2011, Semanario Judicial de la Federación y su Gaceta, Novena Época, XXXIV, p.221.










Reflexiones y conclusiones

Con los intereses en juego, así como los derechos y libertades fundamentales de los individuos, tanto en la UE como en México, es indudable que cualquier Estado debe contar y hacerse de los instrumentos que le permitan —de manera eficaz y respetuosa con los derechos a la vida privada y la protección de datos personales— hacer frente a los retos que la lucha contra la delincuencia organizada y el terrorismo plantean. En especial en un escenario en el cual las comunicaciones electrónicas constituyen herramientas indispensables para todas las partes implicadas. Sin embargo, es indispensable que los instrumentos empleados para garantizar la seguridad de los ciudadanos, respeten y salvaguarden el equilibrio de los derechos y libertades que pueden verse limitados con su adopción.

En otras palabras, los derechos a la privacidad y a la protección de los datos personales no deben ni pueden ceder de forma absoluta frente al derecho a la seguridad. En México, y sin lugar a dudas, las disposiciones de los artículos 189 y 190, fracciones I a IV, de la vigente Ley Federal de Telecomunicaciones y Radiodifusión constituyen injerencias en los derechos a la vida privada y a la protección de datos personales. En todo caso, y sin poner en duda que cada Estado cuenta con la facultad para adoptar las medidas adecuadas y convenientes para asegurar la seguridad de los individuos en función de su realidad histórica y social —con respeto de derechos y libertades fundamentales que en la cultura occidental tienen el carácter de universales—, de todo lo expuesto es posible extraer, al menos, las siguientes conclusiones:

- Cualquier medida que pretenda establecer la conservación y el acceso a los datos personales generados o tratados como resultado de comunicaciones electrónicas constituirá una injerencia en los derechos a la vida privada y la protección de datos personales.
- No toda injerencia en los derechos y libertades fundamentales debe considerarse inválida.
- Sin embargo, cualquier injerencia en los derechos y libertades fundamentales que sobrepase los límites necesarios para alcanzar los objetivos legítimos que se persiguen con su adopción debe considerarse inválida.

Referencias

-  Comisión Europea, Dirección General de Justicia, Protección de Datos. (2013). Web Oficial del Grupo de Trabajo de Protección de Datos del Artículo 29. Recuperado de: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.
-  Comisión Europea. (2012, 25 de enero). Commission proposes a comprehensive reform of the data protection rules. *Data Protection*. Recuperado de: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
-  Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco). *Diario Oficial de las Comunidades Europeas*, 24 de abril de 2002. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2002.108.01.0033.01.SPA.
-  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 (Directiva sobre la privacidad y las comunicaciones electrónicas). *Diario Oficial de las Comunidades Europeas*. 31 de julio de 2002. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2002.201.01.0037.01.SPA.
-  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 de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. *Diario Oficial de la Unión Europea*. 13 de abril de 2006. Recuperado de: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2006.105.01.0054.01.SPA.
-  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. *Diario Oficial de las Comunidades Europeas*, 23 de noviembre de 1995. Recuperado de: <http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:31995L0046>.
-  Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación, 5 de julio de 2010.

- 
-  Ley Federal de Telecomunicaciones y Radiodifusión, *Diario Oficial de la Federación*, 14 de julio de 2014.
 -  Supervisor Europeo de Protección de Datos. (2015). Web oficial del Supervisor Europeo de Protección de Datos. Recuperado de: <https://secure.edps.europa.eu/EDPSWEB/edps/EDPS>.
 -  Tribunal de Justicia de la Unión Europea (sin fecha). Las diversas clases de procedimientos. La cuestión prejudicial. Recuperado de: http://curia.europa.eu/jcms/jcms/Jo2_7024/#competences.
 -  Tribunal de Justicia de la Unión Europea (sin fecha). Presentación general. Recuperado de: http://curia.europa.eu/jcms/jcms/Jo2_6999/.
 -  Tribunal de Justicia de la Unión Europea. (2015). Web Oficial del Tribunal de Justicia de la Unión Europea. Recuperado de: http://curia.europa.eu/jcms/jcms/j_6/.
 -  Tribunal de Justicia de la Unión Europea. *Caso Digital RightsIrelandLtd* y otros (asuntos acumulados C-293/12 y C-594/12). Sentencia de 8 de abril de 2014. Recuperada mediante búsqueda en N° de Asunto "C-293/12": http://curia.europa.eu/jcms/jcms/j_6/.
 -  Tribunal de Justicia de la Unión Europea. *Caso Digital RightsIrelandLtd* y otros (asuntos acumulados C-293/12 y C-594/12). Sentencia de 8 de abril de 2014, apartado 56.
 -  Unión Europea. (2013). Países miembros de la Unión Europea. Recuperado de: http://europa.eu/about-eu/countries/member-countries/index_es.htm.
 -  Unión Europea. (2013). Tratados de la Unión Europea. Recuperado de: http://europa.eu/eu-law/decision-making/treaties/index_es.htm#10.
 -  Unión Europea. (2015). Derecho de la Unión Europea. Reglamento, Directivas y otros actos legislativos. Recuperado de: http://europa.eu/eu-law/decision-making/legal-acts/index_es.htm#30.
 -  Unión Europea. Web oficial de la Unión Europea. (2015). Recuperado de: http://europa.eu/index_es.htm.

