La regulación del respeto a la vida privada y la protección de datos personales en las comunicaciones electrónicas

PID_00250899

Luis De Salvador

Tiempo mínimo de dedicación recomendado: 3 horas

Universitat Oberta de Catalunya

Índice

Introducción

La Propuesta de Reglamento sobre el respeto a la vida privada y la protección de datos personales en las comunicaciones electrónicas (en adelante, para referirnos a él en este texto, utilizaremos el acrónimo de Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas o PRPCE) no puede entenderse como una norma aislada. Esta PRPCE nacerá en el seno de la estrategia del mercado digital (DSM o *digital market strategy*), que tiene como propósito incrementar la confianza de los ciudadanos en los servicios digitales, la seguridad de los datos tratados por los proveedores de servicios y, es importante, la seguridad jurídica de aquellos que despliegan productos y servicios a lo largo del Espacio Económico Europeo.

El mercado digital, no nos engañemos, tiene fronteras, especialmente claras para aquellas empresas que desean desarrollar una auténtica actividad comercial a largo plazo. Actualmente, se han establecido marcos regulatorios distintos dentro de estas fronteras que impiden un despliegue eficaz del mercado único y la libre circulación de información digital, servicios y equipos.

La PRPCE aparece íntimamente ligada al Reglamento general de protección de datos (RGPD o Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos).

Existen diferencias importantes entre ambos, y el título de la PRPCE es significativo ya que marca dos diferencias capitales. La primera es que esta nueva PRPCE se aplica tanto a personas físicas como jurídicas. En este último caso, con el propósito de proteger información de gran valor económico como pueden ser los secretos comerciales e industriales. Como se desarrolla en el Considerando 3, los principios establecidos en el RGPD para las personas físicas se aplican en este caso también a las personas jurídicas, en particular las definiciones, requisitos y límites del consentimiento. Por tanto, las personas jurídicas tienen los mismos derechos como usuarios finales que los atribuidos a las personas físicas y las autoridades de control tienen la obligación de velar por la aplicación de la PRPCE a las mismas, de igual forma que se aplica el RGPD a los usuarios finales.

La segunda es sutil pero importante: la nueva PRPCE establece, explícitamente, su ánimo de proteger tanto la vida privada de los usuarios que utilizan los medios de comunicación electrónicos, en línea a lo establecido en el artículo 7 de la Carta de Derechos Fundamentales de la Unión Europea, como los derechos a la protección de datos de carácter personal de forma coherente con el artículo 8 de la misma Carta y el RGPD. Los conceptos de privacidad y el

de protección de datos de carácter personal son distintos, pero no disjuntos, solapándose en muchos casos y a la vez manteniendo un conjunto de casuísticas independientes. El concepto de protección de datos personales se aplica «al tratamiento total o parcialmente automatizado de dichos datos, algunos no necesariamente íntimos o privados como puede ser el número de DNI, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero», mientras que el concepto de privacidad no está restringido por la consideración de dato personal, el concepto de tratamiento o la inclusión en ficheros.

La PRPCE se encuentra en relación con el RGPD en muchos aspectos como, por ejemplo:

- Pretende regular aquellos aspectos relativos a la protección de datos de carácter personal que surgen en las comunicaciones electrónicas y que no están desarrollados en el RGPD; por tanto, complementa y particulariza algunos principios y derechos en este establecidos, como es el caso de la regulación sobre los datos, identificación y almacenamiento en los terminales móviles.

- Su fecha prevista de entrada en vigor, que será el 25 de mayo de 2018.

- El régimen sancionador hace referencia al desarrollo, en el capítulo VII del RGPD, del mecanismo de coherencia y por tanto su aplicación en el caso de tratamientos trasnacionales.

- Las excepciones a los derechos establecidos en el artículo 23 del RGPD.

- Un nuevo régimen sancionador con puntos en común, etc.

Además, existen otras normas a escala europea con las que pretende y ha de ser coherente, como son:

- La Directiva 2014/53/EU de equipos de radio, que establece, entre otros, la obligación de que en los equipos de radio se incorporen mecanismos que permitan garantizar la privacidad y la protección de los datos de carácter personal de los usuarios.

- El Reglamento europeo de estandarización (EU) 1025/2012, que otorga poderes a la Comisión para establecer medidas en dicho sentido.

- La Directiva (en fase de propuesta) de código europeo de comunicaciones electrónicas que, entre otras, toma en cuenta las OTT (servicios *over the top*, es decir, construidos sobre los servicios ofrecidos sobre otros operadores) y la seguridad de los servicios electrónicos de comunicaciones.

- El Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, en el sentido de que, aunque la PRPCE en estudio no se aplica a las instituciones, cuerpos y agencias de la Unión Europea, la próxima revisión de este tendrá en cuenta lo aquí expuesto en relación con las comunicaciones electrónicas.

1. Cambio de paradigma respecto a la directiva

El marco regulador que hasta ahora, y por ahora, está en vigor en España en relación con las comunicaciones electrónicas, el comercio electrónico y la privacidad en el uso de internet y las redes de datos emana, principalmente, de las siguientes directivas europeas:

- Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas.

- Directiva 2009/136/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, que a su vez modificó la directiva anterior.

- Directiva 2009/140/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (mejor regulación), por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas.

En España, las directivas se traspusieron en dos normas fundamentalmente:

- Ley 9/2014, de 9 de mayo, general de telecomunicaciones (LGT).

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y del comercio electrónico (LSSICE), actualizada mediante Real decreto ley 13/2012, de 30 de marzo, que efectúa la incorporación al ordenamiento jurídico español del nuevo marco regulador europeo en materia de comunicaciones electrónicas; marco que está compuesto por la Directiva 2009/136/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (derechos de los ciudadanos), y la Directiva 2009/140/CE, del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (mejor regulación).

La Comisión Europea, a través de un proceso de revisión crítica de las normas en este sector, llegó a la conclusión de que, si bien los principios y los objetivos de las directivas anteriores permanecen sólidos, en los años transcurridos desde su publicación ha habido un desarrollo tecnológico y de mercado lo suficientemente importante como para ir más lejos que realizar una simple

(1)Voz sobre IP, conjunto de soluciones técnicas que permiten implementar llamadas de voz o de voz y vídeo sobre servicios de internet.

armonización normativa. Estos avances han sido especialmente significativos en el desplazamiento del mercado de los servicios de comunicación masiva, que utilizan los ciudadanos, a servicios de mensajería instantánea, VoIP[1] y servicios de correo electrónico que se construyen sobre la infraestructura de internet y de las compañías herederas de las tradicionales PTT[2].

(2)PTT es un acrónimo que se refiere a las compañías o agencias gubernamentales que tenían el monopolio de las comunicaciones postales, telefónicas y telegráficas, poseedoras de un modelo de negocio y una infraestructura que han heredado las nuevas compañías en el mercado liberalizado.

Estos servicios de mensajería instantánea y de comunicación sobre IP, conocidos por el nombre de OTT, no se encontraban sujetos a lo establecido en las directivas y, por lo tanto, nos encontrábamos ante un vacío normativo que afectaba, por un lado, a los derechos de los ciudadanos, y por otro, a empresas de telecomunicaciones y prestadores de servicios de la información, que se encontraban en una situación de desventaja competitiva.

Además, nos encontramos con un cambio muy importante en el instrumento normativo. Las directivas establecen objetivos para fijar la regulación, pero no definen los medios para llevarlos a cabo. La directiva se había de transponer a la legislación nacional, lo que no siempre ocurría al mismo tiempo en todos los Estados miembros, que fijaba, entre otras cuestiones, el régimen sancionador y que, por tanto, ofrecía un margen más amplio para una implementación distinta en cada uno de los países. Los Estados tienen la obligación de transponer las directivas, pero pueden escoger la norma adecuada (vía legislativa, vía reglamentaria, instrucciones administrativas).

Sin embargo, el reglamento fija tanto los objetivos como los medios y es de aplicación directa en todo su ámbito. El reglamento es esencialmente normativo, obligatorio en todos sus elementos. Desde su entrada en vigor, en la fecha que se fije en su texto, la totalidad de sus disposiciones se imponen a los Estados miembros, a sus jurisdicciones y a los sujetos obligados nacionales, de forma sincronizada en todos ellos.

2. Ámbito y competencia

Mientras que la Directiva 2002/58/CE, y por lo tanto la LSSICE, establecía que su ámbito de aplicación era el tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad Europea, la PRPCE es mucho más amplia.

La PRPCE establece que su ámbito material es el tratamiento de datos de comunicaciones electrónicas llevado a cabo en relación con la prestación y utilización de servicios de comunicaciones electrónicas, así como a la información relacionada con los equipos terminales de los usuarios finales.

Por lo tanto, los aspectos clave de su ámbito de aplicación son:

1) En el ámbito subjetivo:

Se aplica tanto a personas físicas como jurídicas.

2) En el ámbito objetivo:

- Va más allá de los datos de carácter personal, puesto que especifica su competencia sobre los «datos de las comunicaciones electrónicas», definición que veremos más adelante, como se perfila en la PRPCE.

- No se restringe únicamente a las redes públicas de comunicaciones, sino que se extiende a todos los servicios de comunicaciones electrónicas. El cambio que introduce la PRPCE incluye, además, los servicios de comunicaciones como Skype, WhatsApp, Snapchat, etc., y los antes señalados como operadores OTT que no estaban incluidos en la Directiva 2002/58/CE.

- Se amplía la protección no solo a los datos que circulan electrónicamente, sino que se extiende a los equipos terminales de los usuarios finales en su articulado de forma explícita y más extensa a como se establece esa protección en la Directiva 2002/58. De este modo, se da respuesta a una realidad del mercado, que es la complejidad de los teléfonos actuales. Los terminales de los usuarios ya son mucho más que teléfonos, son auténticos ordenadores miniaturizados, de complejidad extraordinaria tanto en los servicios que proporcionan como en la cantidad de información que pueden tratar y almacenar, y se encuentran conectados tanto a la red telefónica como a internet, con capacidades adicionales de comunicación mediante Bluetooth o tecnologías sin-contacto (*contact-less* como NFC) o GPS.

- La utilización de los citados servicios en toda su extensión, en la medida en que puedan aparecer nuevas aplicaciones o servicios que no podamos determinar en este momento.

3) En cuanto al ámbito territorial, este se extiende a:

- La prestación de servicios de comunicaciones electrónicas a usuarios finales en la Unión Europea, inclusive aquellos que no sean de pago, este último establecido expresamente.

- Es importante destacar que dicha protección se extiende a todos los usuarios finales que se encuentren en la Unión Europea. Como en el caso del RGPD, se omite la referencia a que el proveedor de servicios sea una empresa con determinadas características, forma jurídica o lugar de establecimiento, con lo que cambia radicalmente el mecanismo para determinar la competencia. La orientación es la opuesta, centrándose en la localización del usuario final; ni siquiera la competencia se establece porque afecte a nacionales de un determinado país, lo que simplifica la determinación de la competencia para el caso de que el usuario afectado sea una entidad multinacional. Es preciso destacar esa protección a los usuarios finales, que en el texto de la propuesta utiliza el término «en» la Unión Europea (*in* en el texto original en inglés) sin hacer ninguna referencia a que sean ciudadanos, residentes o personas en tránsito por la Unión.

La PRPCE establece una serie de exclusiones, lo que supone trasladar a su texto aquellas que ya estaban previstas en la Directiva 2002/58/CE, como son:

- Las actividades fuera del ámbito de aplicación de las leyes de la Unión Europea.

- Actividades de las autoridades competentes con propósito de proteger la seguridad pública y de perseguir las actividades criminales.

- Política exterior y de seguridad de la UE.

- Los tratamientos de comunicaciones electrónicas llevados a cabo por las instituciones, órganos y organismos de la UE, que tienen su propia normativa.

- Y, como novedad en la PRPCE, se añaden, como excepción, los servicios de comunicaciones electrónicas no accesibles al público, como son las redes de datos corporativas cuyo acceso está limitado exclusivamente a los miembros de la entidad jurídica. Es decir, en principio, no se aplica a una intranet las obligaciones relativas a, por ejemplo, la conservación de datos de la comunicación, o en el caso de un servicio de telefonía interno mediante VoIP los derechos de ocultación y bloqueo de llamadas. Ese tráfico

interno estará regulado en la medida que esa comunicación se extienda al exterior, es decir, a través de internet, a las redes públicas.

Al igual que en el RGPD, se exige a los prestadores que, cuando la entidad no esté establecida en la Unión Europea, dicha entidad ha de nombrar un representante con las siguientes condiciones:

- Ha de ser nombrado por escrito.
- El representante ha de estar establecido en uno de los Estados donde la entidad preste servicios de comunicaciones.
- El representante ha de estar facultado para proporcionar información tanto a las autoridades de control como a los usuarios finales.

La competencia, como determina el artículo 18, para garantizar el cumplimiento de lo establecido en la PRPCE, se remite a la misma autoridad que sea la encargada de supervisar el cumplimiento del RGPD. Esto supone que, en el caso de España, la autoridad competente será, en principio, la Agencia Española de Protección de Datos. En el Considerando 38 de la PRPCE se hace una referencia explícita a que algunos Estados de la Unión dispondrán de más de una autoridad competente para reflejar su estructura administrativa, organizacional o constitucional. Como en el párrafo anterior, acentúa la necesidad de que las mismas responsabilidades otorgadas a las actuales autoridades competentes en el marco del RGPD sea el criterio para asignar dichas competencias en el marco de la PRPCE, y para articular los mecanismos de coherencia. En consecuencia, parece que el criterio para la distribución de competencias entre la AEPD y las actuales autoridades autonómicas será el que se derive de la aplicación del RGPD y se establezca en la nueva Ley orgánica de protección de datos que es objeto de tramitación.

Esto supone una importante novedad respecto a la LSSICE y la LGT, que dan competencia a la AEPD únicamente en determinados aspectos de la Directiva transpuesta (publicidad comercial no solicitada o *spam*, *cookies* y notificación de quiebras) y, por lo tanto, estarán por definir las competencias que quedan atribuidas a la actual Secretaría de Estado de Sociedad de la Información y Agenda Digital (SIAD), antigua SETSI.

3. Tratamiento de los datos de las comunicaciones

Para comprender la PRPCE, hay una serie de definiciones que resultan fundamentales y se desarrollan en el artículo 4. Entre ellas, encontramos las definiciones relativas a:

- **Contenido de la comunicación electrónica:** el contenido intercambiado por el usuario utilizando los medios electrónicos, como son: texto, voz, vídeos, imágenes y sonidos.

- **Metadatos:** datos tratados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas; por ejemplo, los utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del dispositivo generados en el contexto de la prestación del servicio, la fecha, la hora, la duración y el tipo de comunicación.

El contenido y los metadatos, el total de ambos, es lo que se identifica como el conjunto de datos de las comunicaciones electrónicas, y que en el segundo considerando se establece que son, al menos, los números llamados, las webs visitadas, la información geográfica, la fecha, hora y duración de las llamadas realizadas por un usuario final. Toda esta información permite inferir información sobre la vida privada de las personas como son sus relaciones sociales, sus hábitos y actividades en la vida diaria, sus intereses, gustos, etc. Por ejemplo, el análisis de las llamadas frecuentes, y la forma en que se efectúan dichas llamadas, a organizaciones religiosas, partidos políticos, sindicatos o asociaciones militantes pueden proporcionar un perfil sobre las creencias e ideología del usuario final.

Al aplicarse esta protección a las personas jurídicas, hay que realizar un inciso en relación con la importancia que tiene esta información para proteger los intereses de las entidades. Los metadatos son una importante fuente de información con relación a las actividades comerciales y financieras de las empresas. No hay que despreciar en ningún caso su importancia. La monitorización de las mismas, incluso sin acceso al contenido de la comunicación, añadida a la información de fuentes abiertas, puede proporcionar un cuadro muy definido de las actividades y puntos débiles de una actividad empresarial en un momento dado.

También es importante destacar que se ha realizado un cambio de denominación en relación con los datos adicionales recogidos en la implementación de las comunicaciones electrónicas. Hasta ahora, y para ese tipo de datos, se ha estado utilizando la denominación «datos de tráfico y localización» en un conjunto de normativas como:

- La Ley general de telecomunicaciones como en la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

- Las especificaciones técnicas del Instituto Europeo de Normalización de Telecomunicaciones (ETSI).

- La ETSI ES 201 671: «Lawful interception; handover interface for the lawful interception of telecommunications traffic».

- Y la ETSI TS 133 108: «Universal mobile telecommunications system (UMTS); 3G security; handover interface for lawful interception».

De estas dos últimas se derivan las órdenes ministeriales reguladoras de las especificaciones técnicas de los sistemas de comunicaciones electrónicas, que utilizan la misma terminología.

El concepto de metadato introducido en la PRPCE es más amplio que el tradicional de «datos de tráfico», ya que la realidad técnica actual determina que, durante el establecimiento de la comunicación en los sistemas actuales, se pueden recoger infinidad de datos relativos a la naturaleza, tipo, configuración y operación del terminal del usuario.

La PRPCE establece, en su Considerando 15, que los datos de las comunicaciones electrónicas han de considerarse como confidenciales. En consecuencia, cualquier interferencia en la comunicación, tanto por medios automáticos como por medios manuales, debe estar prohibida, siempre que no se tenga el consentimiento de todas las partes implicadas en la comunicación. Por otro lado, en el Considerando 17, se reconoce la importancia que para la actividad económica y para la prestación de servicios en la infraestructura de comunicaciones podría tener el procesamiento de dicha información, intentando buscar un equilibrio en su articulado ambos objetivos.

De esta forma, la PRPCE establece en el artículo 6 cuándo se pueden tratar los datos, es decir, tanto el contenido de la comunicación como los metadatos de las comunicaciones. Los datos se podrán tratar cuando:

- Sea necesario para transmitir la comunicación, y solo durante el periodo imprescindible para implementarla.

- Sea necesario para mantener o restablecer la seguridad o detectar fallos en la comunicación, también solo durante el periodo de tiempo imprescindible para implementarla.

A su vez, establece cuándo se pueden tratar específicamente los metadatos de comunicaciones, extendiendo la posibilidad de tratar ese subconjunto de los datos de la comunicación para los casos que sea necesario determinar:

- La calidad de servicio.

- La facturación.

La PRPCE permite tratamientos adicionales de los metadatos de la comunicación siempre y cuando medie el consentimiento expreso del usuario. Este consentimiento no será general, sino que se podrá otorgar para uno o más fines concretos y definidos, y siempre que los fines o servicios no pueden alcanzarse mediante el tratamiento de datos anonimizados.

También la PRPCE permite extender el tratamiento del contenido de las comunicaciones siempre y cuando:

- Medie el consentimiento expreso de los usuarios finales para la prestación de un servicio específico al usuario. Además solo en el caso de que dicho servicio no se pueda prestar en ningún caso sin acceder al contenido de la comunicación.

- Se recabe el consentimiento de todos los usuarios finales afectados. Esto implica el usuario origen de la comunicación y, por supuesto, el usuario destino de la misma, los dos extremos de la comunicación. Además, ha de especificarse ese consentimiento para uno o más fines concretos, incluyendo la misma condición que para el tratamiento de los metadatos: si no pueden alcanzarse mediante el tratamiento de datos anonimizados.

En este último caso, la PRPCE remite al procedimiento de consulta previa a la autoridad de control establecido en el artículo 36 del RGPD. Aunque no se establece explícitamente en el articulado de la PRPCE, la remisión a dicho artículo del RGPD implica la obligación del proveedor de servicios de comunicaciones de llevar a cabo el equivalente a una evaluación del impacto relativo a la protección de datos o EIPD, como sí se establece en el Considerando 17 de la PRPCE.

La EIPD es un análisis crítico del tratamiento de los datos personales que se llevan a cabo en un proceso, servicio o negocio. Está orientado a identificar tanto los efectos directos y previstos en el objeto de dicho tratamiento como los efectos secundarios, laterales o indeseados que el mismo puede ocasionar a la privacidad, intimidad y libertad tanto de los clientes como de usuarios o terceros. Es un estudio que trasciende el marco local de las actividades de la

propia organización, o los propósitos originales del tratamiento, y ha de adoptar una visión global cuyo objetivo es la protección de los derechos humanos y las libertadas fundamentales tal y como se desarrollan en el RGPD.

En el marco de la PRPCE, este análisis ha de alcanzar no solo a las personas físicas, sino también a las personas jurídicas. Además, estudiando no solo el problema del tratamiento de datos personales en el marco del RGPD, sino además en el marco de la PRPCE, y extendido a la privacidad de los usuarios y de las entidades.

Como nota final de este apartado, es interesante señalar que el Considerando 17 no establece que forme parte de los metadatos aquella información de localización generada por el dispositivo terminal del usuario, pero no recogida en el marco del establecimiento de una comunicación electrónica. Esto supone que todas las aplicaciones que recogen información de localización en, por ejemplo, un *smartphone* quedan fuera de la aplicación de esta normativa mientras que no puedan relacionar la geolocalización recogida con el establecimiento de comunicaciones electrónicas.

4. Almacenamiento y supresión de datos

El almacenamiento y la supresión de los datos relativos a cualquier comunicación es uno de los aspectos más sensibles en relación con la privacidad de los ciudadanos, específicamente su acceso por los distintos Cuerpos de Seguridad del Estado o el propio Gobierno, y con relación a todos los datos de la comunicación, es decir, metadatos y contenido de la comunicación.

En principio, el artículo 7 de la PRPCE establece, de forma genérica, que el contenido de las comunicaciones se suprimirá o anonimizará una vez recibido por el destinatario, y que los metadatos se suprimirán o anonimizarán cuando ya no sean necesarios para transmitir una comunicación. Es importante hacer notar que, en principio, los requisitos de almacenamiento y borrado no son iguales para todos los datos de la comunicación, sino que son más estrictos para el caso del contenido de la comunicación, el elemento más sensible de la misma, que para los metadatos de dicha comunicación.

El propio artículo establece una serie de excepciones al tratamiento de los datos de la comunicación:

- El propio usuario, o una tercera parte bajo sus instrucciones, podrá almacenar o procesar el contenido de la comunicación siempre siguiendo lo establecido en el RGPD.

- Los metadatos, pero no todos, solo aquellos que sean relevantes para cumplir con las obligaciones legales relacionadas con la facturación de los servicios, podrán mantenerse hasta que se extingan las mismas o se pueda reclamar el pago de acuerdo con las distintas leyes nacionales. Esta última anotación establece algunas diferencias en los periodos de retención entre los distintos Estados europeos.

Un aspecto muy interesante y novedoso, como se ha comentado anteriormente, es lo establecido en el artículo 8 en relación con la protección de la información almacenada en los equipos terminales de los usuarios.

Específicamente, el artículo trata de la protección no solo de los datos almacenados en el terminal del usuario, sino también de otros tres aspectos muy interesantes:

- La protección de la información que es posible obtener del terminal del usuario, que es distinta a la información almacenada que se genera durante la utilización de los servicios, y que es relativa a la configuración concreta del equipo terminal (identificadores unívocos asociados a la implementación en ese terminal de sistemas operativos, aplicaciones, servicios,

u opciones de configuración como idioma, región, distribución de iconos, etc.), que se pueden consultar y recoger de forma remota por terceros.

- Las capacidades de almacenamiento del equipo terminal.

- Y, también novedoso y de gran implicación, la protección a las capacidades de proceso de dicho sistema terminal, por lo que no se podrá hacer uso por parte de un proveedor de servicios de las capacidades de proceso de los terminales de sus clientes para implementar servicios más allá de los solicitados por los mismos clientes. Un ejemplo evidente en relación con este tema es el de las *botnets*, conjunto o red de robots informáticos o *bots* descargados en terminales de terceros, que se ejecutan de manera autónoma y transparente para el dueño del terminal y que se controlan de forma remota por el artífice de la misma *botnet*.

Se tratará más sobre este tema más adelante, cuando analicemos las novedades relativas a la regulación de los dispositivos de almacenamiento y recuperación de datos (*cookies*).

En un principio, parece que en el articulado no se establecen directrices con relación a la conservación de datos para acceso por parte de los agentes facultados. Y, en relación con dicho tema, conviene traer a la memoria que la Directiva de conservación de datos de tráfico (2006/24/CE), transpuesta en la Ley 25/2007, fue anulada en 2014 por sentencia del Tribunal de Justicia de la Unión Europea (Sentencia del Tribunal de Justicia de 8 de abril de 2014, Digital Rights Ireland y Seitlinger y otros, asuntos acumulados C-293/12 y C-594/12) en interpretación de la Directiva de ePrivacy y la Carta de Derechos Fundamentales.

Pero, por otro lado, nos encontramos con un artículo 11 en la PRPCE que establece la posibilidad de introducir ciertas limitaciones a las obligaciones y derechos que se describen en el artículo 5, la confidencialidad de los datos de las comunicaciones, el artículo 6, sobre el tratamiento de datos de la comunicación, el artículo 7, sobre el almacenamiento y borrado de los datos, y el artículo 8, de la protección de la información almacenada en los terminales de usuarios.

Este artículo da libertad a los distintos Estados para determinar las limitaciones a los derechos y obligaciones establecidos en la PRPCE que estos consideren oportunos. El artículo habla de «medidas legislativas», sin determinar la categoría de las mismas (ley orgánica, ordinaria o reglamento). Tan solo que dichas medidas estén orientadas a la protección de los intereses listados en las letras de la «a» a la «e» del artículo 23 del RGPD:

- La seguridad del Estado.

- La defensa.

- La seguridad pública.

- La prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención.

- Otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social.

A los que la PRPCE añade la monitorización, inspección o función regulatoria conectada con el ejercicio de las funciones oficialmente encomendadas a una autoridad en relación con dichos intereses.

Por lo tanto, y hasta que no se establezca lo contrario, la Ley 25/2007 de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones fija el marco legislativo en el que se establecen dichas limitaciones a los derechos a la privacidad y obligaciones de conservación que se extienden a los proveedores de servicios de las comunicaciones electrónicas. Y, por otro lado, como se puede ver en el Anteproyecto de Ley orgánica de protección de datos de carácter personal, en el artículo 53.3: «Cuando no haya podido realizar la identificación por otros medios, la Agencia Española de Protección de Datos podrá recabar de los operadores que presten servicios de comunicaciones electrónicas disponibles al público y de los prestadores de servicios de la sociedad de la información los datos que obren en su poder y que resulten imprescindibles para la identificación del presunto responsable de la conducta contraria al Reglamento (UE) 2016/679 y la presente ley orgánica cuando se hubiere llevado a cabo mediante la utilización de un servicio de la sociedad de la información o la realización de una comunicación electrónica». Es decir, se otorgan competencias específicas a la Agencia Española de Protección de Datos para el acceso a los metadatos de las comunicaciones electrónicas para el ejercicio de sus competencias, lo que resulta toda una novedad en el análisis comparado de las competencias otorgadas a otras autoridades de control en el entorno de la Unión Europea.

Es más, explícitamente, en el apartado 2 del mismo artículo de la PRPCE, se establece que los proveedores de servicios de comunicaciones electrónicas deberán establecer procedimientos para responder a las peticiones de acceso a los datos de la comunicación de los usuarios finales por parte de los agentes facultados, de la forma que se haya establecido en el marco legislativo nacional. Dichos procedimientos se encontrarán bajo la supervisión de la autoridad de control, tanto con relación a su implementación como a las solicitudes recibidas y a la base legal para revelar la información.

5. DARD, *cookies*, *fingerprinting* y datos de conexión

Los dispositivos de almacenamiento y recuperación de datos (DARD, como se define en la LSSICE) se han llamado comúnmente *cookies*, aunque esta última denominación es solo un subconjunto de los primeros. Las *cookies* se regulan en la Directiva 2002/58/CE. En particular, en su artículo 5.3, en el que se encontraba la siguiente definición:

> «Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento.»

Una traducción desafortunada de dicha definición se traspuso en nuestra LSSICE, en el artículo 22.2, como:

> «Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.»

El término *dispositivo* no se adecuaba técnicamente a la definición de *cookie*; es confuso, pero, lo que es peor, estaba muy lejos de la definición de la implementación de las técnicas de *fingerprinting* y otras técnicas que permiten la recogida de información, el seguimiento de los terminales de los usuarios finales y, por tanto, el perfilado de los mismos.

La PRPCE, en su artículo 8, anteriormente citado, identifica dichas técnicas con mayor propiedad al definirlas como «información almacenada en, e información relacionada con el terminal del usuario» en el título del mismo. Esta definición se extiende y es más específica en la enunciación del apartado 1, donde establece las condiciones de uso de las capacidades de almacenamiento y proceso del terminal, incluyendo información sobre su hardware y software. De esta forma cubre tanto las técnicas de *cookies*, *flash cookies*, almacenamiento HTTP, otras técnicas de almacenamiento de información o *tokens* en los equipos terminales, identificadores del hardware o del sistema operativo, *fringerprinting* y cualquier otra que recoja o analice información del dispositivo o de un elemento que procese información en el mismo y que tenga el mismo objeto.

La PRPCE establece, en su Considerando 15, que una intercepción de las comunicaciones se producirá también cuando un tercero ajeno a la comunicación monitorice los sitios web visitados, la fecha, hora y frecuencia de dichas visitas, la interacción con otros, etc.

Por tanto, en su artículo 8.1, prohíbe el uso de técnicas para la recogida de dicha información si no se cumplen las condiciones que ya se determinaban en la Directiva, pero añadiendo una posibilidad adicional al tratamiento, que es su uso para analítica web por parte del propio prestador del servicio de comunicaciones electrónicas, no de un tercero.

En cuanto a las direcciones de internet, IP en sus distintas versiones, y otros identificadores de red, como direcciones MAC, los números IMEI (*international mobile station equipment identity* o identidad internacional de equipo móvil), IMSI (*international mobile subscriber identity* o identidad internacional del abonado a un móvil) y otra información de conexión, como aquella que habitualmente se almacena en los ficheros de *log*, que se señalan en el apartado segundo del mismo artículo como «la recogida de información emitida por el equipo terminal para permitir la conexión con otro equipo u otro equipo de red», se establece la prohibición de su recogida y tratamiento si no es con el propósito de:

- Realizar el establecimiento de conexión.

- Cuando se advierta e informe conforme al RGPD en relación con la finalidad, responsables, etc.).

Además, en la recogida y almacenamiento de dichos datos, han de implementarse medidas de seguridad conformes a lo establecido en el RGPD, es decir, que es necesario llevar a cabo un análisis de riesgos en relación con las medidas de seguridad a seleccionar.

De forma adicional, la PRPCE establece la posibilidad de que se regule la información proporcionada a los usuarios mediante iconos estandarizados.

6. Navegadores

La PRPCE regula ciertas opciones técnicas para obtener el consentimiento de los usuarios finales, en particular con relación al tratamiento de la información recogida en el marco del artículo 8, a través de las *cookies* y de los datos necesarios en el establecimiento de la conexión.

Por un lado, el artículo 9.2 establece que, con relación a la obtención del consentimiento para el tratamiento de *cookies* (llamemos así a las técnicas definidas en el artículo 8.1 para simplificar), se puede considerar un consentimiento válido el expresado por el usuario a través de sus elecciones en las opciones de configuración definidas en el navegador. Por supuesto, hay más herramientas que comunican o intercambian datos a través de la red, no solo los navegadores web; por lo tanto, dicho artículo se aplica también a dichos productos o servicios.

Las obligaciones técnicas se desarrollan en el artículo 10. El apartado 1 impone a los navegadores, y como en el caso anterior también a cualquier utilidad de acceso a internet, la obligación de ofrecer en sus opciones de configuración la posibilidad de impedir a terceros el uso de *cookies*. Es importante resaltar que no solo son los navegadores los obligados a implementar dichas medidas, sino también, por ejemplo, los modernos sistemas operativos que, por defecto, recogen abundante información de los dispositivos de los usuarios.

El apartado 2 establece la obligación de ofrecer, durante el proceso de instalación de las aplicaciones, opciones de configuración de privacidad que han de aprobarse de forma explícita por el usuario antes de continuar con la misma. Incluso, el apartado 3 impone el 25 de agosto de 2018 como fecha límite de actualización para los programas instalados.

Como reflexión final, ante lo desarrollado en el presente apartado sobre los navegadores y el apartado anterior sobre *cookies*, se echa en falta la regulación de los destinatarios finales de la información recogida mediante dichas técnicas, es decir, de las redes de publicidad. Estas son las entidades que están detrás de los beneficios que soportan la mayor parte de los servicios actuales de internet, y que recogen la mayor información posible de los usuarios finales para, mediante la ejecución de procesos que están fuera del control de esta regulación, ofrecer publicidad personalizada gracias al perfilado de los destinatarios de los servicios ofrecidos en la red.

7. Controles concedidos a los usuarios

El capítulo III de la PRPCE establece un conjunto de nuevos controles sobre las comunicaciones electrónicas que se consideran derechos de los usuarios, tanto si se trata de personas físicas como jurídicas.

El primer control que se ofrece a los usuarios está en relación con la identificación de llamadas, siempre y cuando este servicio se proporcione por el proveedor de servicios de comunicaciones electrónicas. Los derechos son:

- La ocultación del teléfono llamante por parte del iniciador de la comunicación.

- Por otro lado, el poder evitar la ocultación del teléfono llamante, control que ha de poder efectuar el receptor de la llamada, y por lo tanto, la posibilidad de que no lleguen las llamadas ocultas por parte de que aquellos usuarios que hayan ejercido el primero de los controles.

- Que el llamado pueda ocultar al llamante la línea con la que este último se ha conectado de forma efectiva.

- El poder establecer el bloqueo de las llamadas entrantes procedentes de determinados números o de fuentes anónimas.

Todos estos controles han de ofrecerse de forma gratuita. Además, estos controles se anularán en el caso de que se realicen llamadas a servicios de emergencia. También se establece que los derechos al control de la ocultación del identificador del llamante se pueden limitar por ley en cada uno de los Estados miembros.

Otro de los controles que se han de ofrecer a los usuarios finales son aquellos relativos al bloqueo de las llamadas entrantes, que se encuentra sujeto a las siguientes consideraciones:

- Se ha de poder realizar el bloqueo de llamantes específicos o de las llamadas anónimas.

- Ha de ser posible detener las llamadas desviadas automáticamente por un tercero al equipo terminal del usuario final.

En cuanto a las guías de abonados de usuarios finales, se establecen las siguientes posibilidades de control:

- Un control *a priori*, como es la necesidad del consentimiento explícito del usuario final para cada uno de los datos que se incluyan en la guía.

- La posibilidad del ejercicio del derecho a objetar sobre su inclusión, y verificar, corregir y eliminar los mismos.

- Un aspecto novedoso es el deber de ofrecer a las personas jurídicas la posibilidad de oponerse a la introducción de sus datos en la guía.

En relación con las comunicaciones comerciales no solicitadas, tanto la Directiva como la LSSICE prohíben el envío de comunicaciones comerciales por medios electrónicos a personas físicas y jurídicas. En este punto la PRPCE introduce una novedad, ya que solo prohíbe los envíos a personas físicas, mientras que establece que los Estados miembros velarán para que las personas jurídicas estén suficientemente protegidas. Por lo tanto, la regulación para los envíos a personas físicas no tiene cambios.

En el caso de las llamadas de venta directa, estas deberán:

- Mostrar una línea con la que se pueda contactar.

- Mostrar un código o prefijo específico definido por la Comisión Europea que permita identificarlas.

El capítulo termina con un artículo, el 17, sobre la información sobre riesgos de seguridad detectados por los proveedores de servicios de comunicaciones electrónicas. En él se establece que, cuando un riesgo en particular pueda comprometer la seguridad, se ha de informar a los usuarios finales sobre el mismo y de las medidas que, en su caso, pueden adoptar los propios usuarios más allá de las que pueda imponer el mismo proveedor, indicando el coste estimado de las mismas.

En esta redacción se echan de menos varios aspectos. En primer lugar, la brevedad y la falta de concreción del mismo. Al referirse a «riesgo», no se establece si este riesgo es alto o bajo. Además, la terminología «riesgo» resulta ambigua, ya que no se hace referencia a si se trata de un riesgo intrínseco, previo a la adopción de medida preventivas, o del riesgo residual. En sí mismo, el término riesgo evita el pronunciarse sobre si la amenaza que puede comprometer la seguridad de los usuarios finales se ha materializado o no.

El segundo aspecto que se echa de menos es el de una referencia explícita a los artículos 33 y 34 del RGPD, en los que se establece la obligación de notificación de violaciones de seguridad a la autoridad de control, y las condiciones para la notificación de las violaciones a los usuarios finales.

El aspecto final que se echa en falta es la definición de qué hechos suponen un compromiso a la seguridad. Si para la definición de un compromiso a la seguridad nos remitimos a la definición establecida en el artículo 4 apartado 12 del RGPD:

> «12) "violación de la seguridad de los datos personales": toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.»

Resulta preocupante que en dicha definición no aparezcan explícitamente definidos los ataques por denegación de servicio que son tan críticos en los servicios de comunicación electrónica y que pueden afectar de forma grave a los usuarios finales, con modelos de ataque desconocidos hasta ahora y que se están extendiendo, como es el caso de los ataques basados en *ramsonware* o cifrado malicioso de los sistemas de información.

Ataques por denegación de servicio

En tecnologías de la información, un ataque de denegación de servicio, también llamado ataque DoS (de *denial of service*), es un ataque a un sistema de computadoras o a una red de comunicaciones que causa que un servicio o recurso (datos, almacenamiento o computación) sea inaccesible a los usuarios legítimos.

8. Multas y sanciones

A diferencia de la Directiva 2002/58/CE, que no establecía un régimen sancionador y que, en cambio, sí establecía la LSSICE y la LGT, la nueva PRPCE establecerá un régimen sancionador. Además, remite al RGPD en varios aspectos:

- El primero con relación a los derechos frente a la autoridad de control establecidos en el RGPD, como son el de presentar una reclamación, el de la tutela judicial efectiva contra la misma autoridad de control, de tutela contra un responsable o encargado del tratamiento y el derecho a la indemnización y responsabilidad de los daños y perjuicios. En este caso, se extienden a todos los usuarios finales, incluyendo personas jurídicas.

- El segundo es el relativo a los mecanismos de cooperación y coherencia que se establecen en el capítulo VII del RGPD, lo que introduce una gran novedad en la tramitación de los procedimientos sancionadores que se realizarán de acuerdo con el mismo.

Como se desarrolla en el Considerando 38, para asegurar la consistencia con el RGPD, el propósito es que las mismas autoridades de control que se consideren competentes para aplicar los principios de protección de datos de carácter personal, en el caso de tratamientos transnacionales, sean las que sean competentes para velar por la aplicación de la PRPCE. En principio, supone la existencia de una autoridad de control principal y la obligación de cooperación con las autoridades de control interesadas, el establecimiento de mecanismos de asistencia mutua y la posibilidad de realización de operaciones conjuntas de las autoridades de control.

Al no establecer criterios en la PRPCE para la determinación de cuál será la autoridad de control principal, se puede inferir que se seguirán los criterios establecidos en el artículo 56 del RGPD, aunque no haya una referencia expresa al mismo.

Además, como en el RGPD, mientras que hay un procedimiento definido para la determinación de las responsabilidades de las autoridades de control cuando el proveedor de servicios tiene al menos un establecimiento en algún territorio de la Unión, no se detalla este procedimiento cuando el proveedor no tiene un establecimiento, sino solo un representante en uno de los Estados. Este es el caso de muchos de los servicios OTT de comunicaciones electrónicas que incluye la regulación de la PRPCE.

En cuanto a las sanciones, la PRPCE establece multas de 10.000.000 de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocios anual total a escala mundial del ejercicio financiero anterior, optándose por la de mayor cuantía en los casos en que las infracciones sean relativas a:

- (art. 8) *Cookies* y *fingerprinting*
- (art. 10) Información y opciones de navegadores
- (art. 15) Directorios públicos
- (art. 16) Comunicaciones no solicitadas

Asimismo, establece multas de 20.000.000 de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocios anual total a escala mundial del ejercicio financiero anterior, optándose por la de mayor cuantía para los casos de infracciones relativas a:

- (art. 5) Confidencialidad de las comunicaciones
- (art. 6) Tratamiento permitidos de datos de comunicaciones
- (art. 7) Almacenamiento y supresión
- (art. 18) Incumplimiento de una orden la autoridad de control

Deja fuera de la norma el régimen sancionador de las infracciones de los artículos 12 a 14 y 17, es decir, los relativos a la identificación de llamadas, al bloqueo de llamadas entrantes y a la información sobre los riesgos de seguridad. En ese caso, el régimen sancionador se deja en manos de los Estados miembros.

A diferencia del RGPD, y sin una referencia explícita al mismo en este aspecto, se echa en falta la enumeración de un conjunto de criterios para graduar la sanción. En una normativa en que la sanción mínima es de cero euros y se extiende hasta cantidades que alcanzan la veintena de millones de euros, la no existencia de criterios de graduación es una fuente de inseguridad jurídica para los administrados y de inseguridad también para las autoridades de control.

Más todavía teniendo en cuenta que se han de implementar mecanismos para una aplicación coherente de la PRPCE en todos los países de la Unión, como explícitamente se establece al introducir una referencia al capítulo VII del RGPD, de una forma u otra tendrán que establecerse criterios comunes para

que todas las autoridades apliquen, de forma homogénea, el régimen sancionador y no nos encontremos con una gran diferencia en la aplicación de la presión administrativa entre los distintos países.

Finalmente, el artículo 22 establece el derecho de indemnización de los usuarios que hayan sufrido perjuicios materiales o morales, salvo que el infractor no sea responsable del hecho que da lugar al perjuicio.

9. Armonización

El espíritu de la PRPCE es el de disponer de un marco común para la aplicación de las mismas reglas de juego en el sector de las telecomunicaciones y del comercio electrónico en todo el espacio económico europeo, incluso más allá de las fronteras del mismo, en aquellos países que se adhieran a los mismos principios.

En un sector en tan rápida evolución y con aplicaciones llenas de matices se hace necesario algo más que una norma común. Es muy difícil encontrar situaciones o comportamientos que se encuentran completamente descritos en los artículos y siempre van a estar sujetos a la interpretación para el caso concreto. Un caso en particular será el de la aplicación del régimen sancionar, con las horquillas tan amplias que existen para la imposición de sanciones.

Por ello, más allá de los mecanismos de coherencia establecidos en el RGPD y en relación con los mismos, se hace necesaria la existencia de un organismo supranacional que permita resolver las discrepancias interpretativas. Esta tarea la asume el Comité Europeo de Protección de Datos, que tiene como misiones específicas:

- Velar por la aplicación coherente de la PRPCE.
- Examinar cuestiones relativas a la aplicación de la PRPCE.
- A su vez, podrá elaborar guías directrices y recomendaciones en relación con aspectos específicos detallados en el mismo.

Si, por un lado, la existencia de la PRPCE y las tareas citadas del Comité Europeo de Protección de Datos son un impulso a la armonización, todavía existe un conjunto de fuerzas centrífugas con relación a la aplicación de un criterio común que siguen operando en este sector.

En primer lugar, la existencia de un reglamento de aplicación directa no implica necesariamente que no se vaya a desarrollar un texto legislativo español. Un texto que permita ajustar los aspectos de la regulación del sector de las telecomunicaciones y del comercio electrónico a las peculiaridades del mercado español o en relación con los aspectos que no han sido desarrollados, o desarrollados parcialmente en la PRPCE. Este texto cubriría, por ejemplo, las limitaciones que se pueden establecer en el control del identificador de la llamada o aquellos relativos al régimen sancionador de las infracciones de los artículos 12 a 14 y 17, es decir, los relativos a la identificación de llamadas, al bloqueo

de llamadas entrantes y a la información sobre los riesgos de seguridad. En ese caso, será necesaria una norma que adecue la cantidad de las sanciones a lo establecido por la PRPCE en el resto de infracciones.

Un antecedente o ejemplo de norma nacional desarrollada en el marco de un reglamento europeo lo encontramos en el actual desarrollo de una nueva ley orgánica de protección de datos a la sombra del RGPD que regulará aspectos complementarios, que no accesorios, en relación con temas de videovigilancia o de ficheros de solvencia. Asimismo, también se contemplan aspectos relativos al ejercicio de la competencia de las autoridades de control, además de temas específicos procedimentales que van a tener una incidencia directa o indirecta en la PRPCE bajo estudio, como puede ser el caso de acceso, por parte de la Agencia Española de Protección de Datos, a los metadatos de las comunicaciones.

A esto se añade la invocación a que los Estados miembros y las autoridades de control tengan en especial consideración las necesidades de las micro, pequeñas y medianas empresas, como señala el Considerando 39 de la PRPCE. Teniendo en cuenta la complejidad de la nueva normativa, tanto de la propuesta de la PRPCE como del RGPD, resulta altamente positivo que se tenga en cuenta, pero no se determine en qué aspectos se va a producir, la concreción necesaria para dar una seguridad jurídica a dichas entidades, y con garantías de que se dé la misma protección a dicha base empresarial en todos los Estados miembros.

Otra de esas fuerzas diferenciadoras entre países deriva de la aplicación de normas ya existentes, como por ejemplo la Ley 25/2007 de conservación de datos de tráfico, en donde se establecen periodos de retención de doce meses para los operadores de telecomunicaciones, que ahora se extiende a todos los proveedores de servicios de comunicaciones. Será interesante ver cómo se materializan estos requisitos en proveedores que ofrecen servicios trasnacionales y que tendrán que adecuar sus servicios a las peculiaridades nacionales.

Por otro lado, es importante no olvidar la aplicación de la Ley 39/2015 y la Ley 40/2015 que regulan el procedimiento administrativo en España, en particular el procedimiento administrativo sancionador, y las leyes procesales penales en los temas con una vertiente criminal. Estos marcos procedimentales son diferentes, y a veces muy distintos, en cada uno de los países europeos: establecen periodos de caducidad diferentes, distintas etapas en los procedimientos y distintos derechos a los interesados en los mismos. Más aún, las diferencias procedimentales se acentúan ante la posibilidad de imponer multas, cuando hay países que, por restricciones constitucionales, no pueden imponer sanciones administrativas y tienen que hacer uso de las vías civiles y penales para su imposición, como reconoce la propia PRPCE en su artículo 23, apartado 8.

Tanto en la aplicación de la propuesta de la PRPCE como en el ya referido RGPD 679/2016, se abre un interesante periodo en el que nos vemos abocados a una *terra incognita* procedimental, en particular cuando se apliquen en los primeros casos que lleguen a las autoridades de control los mecanismos de coherencia y a la hora de determinar los criterios de graduación de las sanciones administrativas.

Bibliografía

BEREC (2016). «Report on OTT services». BoR (16)35.

<http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services>

De Streel, A.; Larouche, P. (2016). *An integrated regulatory framework for digital networks and services, Centre on Regulation in Europe.*

<http://www.cerre.eu/publications/integrated-regulatory-framework-digital-networks-and-services-0>

Gori, P; Parcu,P. L. (2015). «Electronic communications policy and regulation in Europe». En: C. Jaag; M. Finger. *The Routledge companion to network industries* (págs. 141-155). Taylor Francis.

Policy Department A (2015). Economic and Scientific policy, Over-the-Top players (OTTs), Directorate- General for Internal Policies, European Parliament, PE 569.979.

Policy Department A (2016). Economic and Scientific policy, Reforming EU telecoms rules to create a Digital Union, Directorate-General for Internal Policies, European Parliament, PE 570.011.

Rossi, L. (2015). *Proposal for the reform of the regulation of digital services*. Robert Schuman Centre, European University Institute.

Schrefler, L. (2016). *Reforming the regulatory framework for electronic communications networks and services – Implementation Assessment, EPRS.*

<http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2016)581400>