ARI 92/2018
24 de julio de 2018

Privacidad, confidencialidad e interceptación de las comunicaciones

Javier Alonso Lecuit | Miembro Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

Tema

La UE y sus Estados miembros han elaborado nuevas propuestas de regulación para proteger la confidencialidad de las comunicaciones electrónicas, interceptar esas comunicaciones en el curso de investigaciones policiales y judiciales y acceder a pruebas electrónicas.

Resumen

La UE y sus Estados miembros afrontan un proceso regulatorio para asegurar la confidencialidad de las comunicaciones electrónicas de los individuos y empresas y posibilitar la obtención de pruebas electrónicas en los entornos on-line. La regulación trata de cubrir el vacío legal en el que se encuentran los productos y servicios de comunicaciones electrónicas ofrecidos por los proveedores de Internet y las dificultades que plantea la disruptiva evolución tecnológica a las fuerzas de seguridad y las autoridades judiciales para desarrollar sus investigaciones y obtener pruebas en el ciberespacio.

Entre las iniciativas de regulación se encuentran las llevadas a cabo por la Comisión para proteger derechos y libertades fundamentales como la privacidad, confidencialidad y los datos de carácter personal en el sector de las comunicaciones electrónicas (Reglamento e-Privacy) en línea a la regulación horizontal de los datos de carácter personal (Reglamento General de Protección de Datos, RGPD) y el acceso a pruebas electrónicas y datos almacenados en el curso de investigaciones transfronterizas en la UE (Reglamento e-Evidence). Del mismo modo, países como el Reino Unido, Francia o España han actualizado su legislación en materia de interceptación legal para adaptarla a las nuevas plataformas on-line de la sociedad de la información y a las necesidades operativas de las fuerzas de seguridad.

La regulación incluye elementos controvertidos como la interceptación individualizada o masiva de las comunicaciones, el cifrado extremo a extremo de las comunicaciones, la retención de datos y metadatos, la infiltración, registro y extracción remota de información de dispositivos, el bloqueo o borrado de contenidos ilegales de servidores la identificación en tiempo real de amenazas o el perfilado de ciudadanos y organizaciones potencialmente sospechosas.

Análisis

La protección de los datos de carácter personal y la confidencialidad de las comunicaciones electrónicas

La propuesta para la actualización de la Directiva 2002/58/CE sobre privacidad y comunicaciones electrónica tiene por objeto garantizar la privacidad, la confidencialidad y la protección de los datos personales de las comunicaciones electrónicas en amparo de los derechos y libertades fundamentales de las personas físicas y jurídicas. Trata de adecuarla a los profundos cambios tecnológicos y de modelos de negocio on-line que permiten comunicaciones interpersonales (entre otros, servicios de voz sobre IP, de mensajería instantánea o de correo electrónico basados en la web) que son en ocasiones funcionalmente equivalentes a los ya regulados como la telefonía o los mensajes SMS.

La Directiva e-Privacy de 2002 sólo protege los servicios tradicionales de comunicaciones de voz/texto y el servicio de acceso a Internet ofrecidos por las compañías de telecomunicaciones, pero no se aplica a los nuevos servicios de comunicaciones on-line (over-the-top, OTT) ofrecidos por los proveedores de la sociedad de la información a través de Internet, en lugar de los operadores tradicionales. Esto plantea una importante asimetría regulatoria entre operadores que prestan servicios equivalentes, ya que, por ejemplo, los operadores de telecomunicaciones únicamente pueden procesar la información vinculada a las comunicaciones con el estricto consentimiento del usuario caso a caso, a diferencia de los OTT que pueden hacerlo sobre una base de consentimiento más amplia tal y como establece el RGPD.

La Comisión atribuye la necesidad de revisión a algunos factores como la desprotección de la privacidad y la confidencialidad en las comunicaciones on-line; la obsolescencia tecnológica; la ineficacia de las reglas de consentimiento en la gestión de *cookies*; la falta de regulación de mecanismos *on-line* alternativos a las *cookies* como la huella digital de los terminales o el uso del identificador MAC del dispositivo al conectarse a redes wifi y bluetooth; la indefinición de la Directiva en relación con las comunicaciones de datos entre dispositivos M2M/IoT o la desprotección de los ciudadanos frente a comunicaciones no solicitadas en campañas de telemarketing. La Comisión argumentaba estos y otros factores en su Evaluación del Impacto de la actualización para justificar su revisión.

Como resultado, la Comisión presentó en enero de 2017 una propuesta de Reglamento para respetar la privacidad y la protección de los datos personales en las comunicaciones electrónicas (Reglamento e-Privacy) que se encuentra actualmente en tramitación. La propuesta se formalizó como Reglamento, en lugar de como Directiva, para evitar las dilaciones de su trasposición, garantizar la coherencia con el RGPD, armonizar la protección de los usuarios y abaratar los costes de las empresas que desarrollan actividades transfronterizas. La propuesta del Reglamento e-Privacy, que ya incorpora a los operadores OTT, será de aplicación en el tratamiento de datos de las comunicaciones electrónicas incluidas en ella (las cuestiones que no se contemplen específicamente en la propuesta, quedan amparadas por el RGPD) como a la información procesada y almacenada en los terminales de los usuarios. No se aplicará a las actividades llevadas a cabo por las autoridades competentes en la prevención,

investigación, detección o enjuiciamiento de infracciones penales, incluida la protección y prevención frente a amenazas para la seguridad pública.

En concreto, el Reglamento prohíbe cualquier interferencia con las comunicaciones electrónicas, es decir, la escucha, el almacenamiento, el seguimiento, el análisis u otros tipos de interceptación, la vigilancia o el tratamiento de datos de las comunicaciones. Autoriza a los proveedores de redes y servicios de comunicaciones el tratamiento de datos y contenidos de comunicaciones electrónicas cuando sea necesario para llevar a cabo la comunicación durante el período necesario, con el fin de mantener o restablecer la seguridad de las redes y servicios o detectar fallos técnicos en la transmisión de las comunicaciones electrónicas, todo ello durante el tiempo necesario para estos fines.

Los proveedores podrán tratar los metadatos de comunicaciones electrónicas (son datos tratados en la red con el fin de transmitir, distribuir o intercambiar contenido de comunicaciones electrónicas, incluyendo los utilizados para rastrear e identificar el origen y el destino de una comunicación, la ubicación del dispositivo generados en el contexto de la prestación de servicios de comunicaciones electrónicas, así como la fecha, la hora, la duración y el tipo de comunicación) cuando sea necesario para cumplir con las obligaciones de calidad del servicio, facturar, calcular las tarifas de interconexión, detectar o impedir la utilización abusiva o fraudulenta de los servicios, o prestar servicios específicos al usuario. También podrán tratar los contenidos (formatos de texto, voz, vídeos, imágenes y audios) de comunicaciones electrónicas. En ambos casos, será preciso el consentimiento para fines concretos de los usuarios y el tratamiento anonimizado de la información.

Los proveedores suprimirán el contenido de las comunicaciones o los anonimizarán una vez recibidos por los destinatarios o cuando ya no sean necesarios para transmitir la comunicación (podrán conservarse los metadatos asociados a la facturación hasta que finalice el plazo de reclamación). La propuesta permite el tratamiento, almacenamiento y recopilación de la información almacenada en las terminales si el usuario ha dado su consentimiento, o para efectuar la transmisión de una comunicación, cuando sea necesario para la prestación de un servicio on-line solicitado por el usuario final o para medir la audiencia en la web, siempre que corra a cargo del proveedor que haya solicitado por el usuario final.

La propuesta prohíbe recopilar la información emitida por un terminal para poder conectarse a otro dispositivo o a un equipo de red (por ejemplo, wifi o bluetooth) salvo para establecer una conexión y durante el tiempo necesario para ello. Establece que los programas que permiten comunicaciones on-line, incluyendo los navegadores habrán de ofrecer la posibilidad de impedir a terceros almacenar información sobre el terminal del usuario o el tratamiento de información ya almacenada en ese equipo. Además, actualiza los derechos de personas físicas y jurídicas al control de las comunicaciones tales como la presentación y restricción de la identificación o el bloqueo de llamadas entrantes, las guías accesibles al público o comunicaciones no solicitadas.

Los operadores tradicionales de telecomunicaciones han apoyado la inclusión de los nuevos operadores OTT pero asociaciones importantes del sector como GSMA y ETNO han mostrado en su valoración reservas sustanciales en relación con las estrictas reglas planteadas por la Comisión para el procesado de los metadatos asociados a las

comunicaciones y, en particular, a los relativos a la localización o a la pormenorización del consentimiento que estarán obligados a solicitar a los usuarios En su lugar, GSMA y ETNO proponen flexibilizar el procesado de los metadatos de las comunicaciones electrónicas adoptando principios similares a los establecidos en el Reglamento General de Protección de Datos como los de responsabilidad proactiva (accountability) y protección por diseño con técnicas tales como la pseudo-anonimización o el cifrado de los mismos.

En particular, causa especial preocupación a los operadores las restricciones relativas al uso de metadatos no anonimizados para llevar a cabo la gestión de los recursos técnicos de las redes de telecomunicaciones, por ejemplo, limitadas en el borrador al cumplimiento de los requisitos de calidad de servicio "obligados", máxime si se tiene en cuenta que la calidad de servicio es un elemento base para la diferenciación competitiva de los servicios ofrecidos entre los distintos operadores de red. Restricciones que también afectarían a la próxima generación de redes móviles 5G si sólo se permite el análisis de datos de tráfico anonimizados, limitando las capacidades de planificación técnica, el seguimiento pormenorizado de anomalías o la asignación dinámica y automática de los recursos técnicos de la red, por ejemplo, adaptando la dirección de los haces de las antenas de las estaciones base según los requisitos particulares de los usuarios. Además, la rigidez regulatoria en relación con el consentimiento resulta poco compatible con una explotación eficiente de los datos (big data) mediante herramientas analíticas, por ejemplo, en plataformas destinadas a *smart-cities* o en aplicaciones industriales M2M/IoT ("Industria 4.0") a las que también aplicaría el principio sobre la confidencialidad de las comunicaciones que propone el Reglamento.

Medidas regulatorias de la UE y de los Estados miembros para la interceptación de las comunicaciones para apoyar las investigaciones de las autoridades policiales y judiciales

Entre los temas en discusión en este ámbito se incluyen elementos tan diversos como las bases legales que permiten la interceptación individualizada y masiva de las comunicaciones, el acceso a terminales y comunicaciones cifradas extremo a extremo, el registro remoto de dispositivos, extracción de información, infiltración, la identificación en tiempo real de amenazas, el acceso a pruebas electrónicas, el bloqueo o borrado de contenidos ilegales de servidores o el periodo de retención de datos y metadatos, entre otros. Son instrumentos que la regulación vigente (Reglamento 2016/679 y Directivas 2016/680 y 2016/681) exige se apliquen de forma selectiva y proporcional a la naturaleza y gravedad de los delitos investigados, así como un tratamiento de los datos personales conforme a derecho.

Su actualización es necesaria porque los servicios de comunicaciones tradicionales ofrecidos por operadores de telecomunicaciones nacionales han ido evolucionando hacia un escenario global formado por aplicaciones on-line ofrecidas por los proveedores de Internet (OTT) ya mencionados y disponibles a través del servicio de acceso a Internet proporcionado por los operadores de telecomunicaciones locales a través de redes fijas (fibra y xDSL) y móviles, a lo que hay que añadir el despliegue de redes móviles 5G y la virtualización de las infraestructuras de comunicaciones. Un cambio de escenario que afecta a la interceptación de las comunicaciones.

En el pasado, los servicios de telecomunicaciones estaban constituidos esencialmente por el servicio telefónico, la mensajería SMS y los servicios portadores de datos. La inteligencia de estos servicios residía en la red y el operador gestionaba extremo a extremo la comunicación del usuario. Las comunicaciones de datos se ofrecían a las corporaciones habitualmente mediante circuitos punto a punto o estableciendo redes privadas virtuales, el cifrado extremo a extremo tenía un uso marginal. El intercambio internacional de datos era comparativamente reducido, la intercepción se realizaba a un nivel local en la red del operador de telecomunicaciones.

En la actualidad, la inteligencia del servicio reside en los extremos, es decir en los terminales de usuario y en las aplicaciones de Internet, y cada operador de telecomunicaciones tiene control únicamente sobre su red (un segmento de la comunicación de Internet). La mayor parte de las comunicaciones (voz IP, mensajería, redes sociales, video...) se realizan en Internet y solo una parte de los contenidos de la Red es visible a través de buscadores. Además, las aplicaciones han recurrido al cifrado entre los extremos de la comunicación para proteger el contenido de las comunicaciones.

Este cambio estructural experimentado por el mercado de las comunicaciones electrónicas ha tenido importantes efectos en la interceptación judicial y policial de las comunicaciones de los sujetos investigados. Ya no es suficiente con tener acceso al servicio de conectividad (la comunicación vocal o el acceso de datos a Internet ofrecido por el operador local de telecomunicaciones), surge la dificultad de solicitar la intervención a proveedores emplazados en terceros países o la imposibilidad de descifrar comunicaciones y terminales. Por otra parte, Internet ha provocado una concentración e internacionalización del tráfico de datos, propiciando la captura masiva de metadatos en tiempo real.

El uso por la delincuencia organizada y por el terrorismo internacional de las aplicaciones más populares de Internet, como redes sociales y servicios de comunicaciones vocales cifrados, con fines de propaganda y comunicación segura entre sus miembros así como la extraterritorialidad del ciberespacio forman parte central del debate legal sobre la necesidad de regular ciertas prácticas de Internet, tales como el uso del cifrado extremo a extremo o la eliminación de determinados contenidos en redes sociales, así como la corresponsabilidad de los proveedores de Internet.

Lo anterior ha llevado al Consejo Europeo de junio de 2016 a solicitar una mayor cooperación en las investigaciones criminales entre las autoridades policiales y judiciales y los proveedores de servicios de comunicaciones electrónicas, especialmente a aquellos proveedores de Internet no establecidos en la UE. Por su parte, la Comisión aprobó en 2018 una Directiva 2017/541 para la lucha contra el terrorismo, cuyo plazo de trasposición vence en septiembre de 2018 que los Estados colaboraran para evitar la comisión de delitos de terrorismo desde los servidores ubicados en su territorio, procurando obtener la eliminación cuando los contenidos estén albergados fuera de su territorio y, si no fuera factible su eliminación en origen, utilizar mecanismos que bloqueen el acceso a los mismos desde el territorio de la UE. No obstante, la Directiva advierte que no debe imponerse a los proveedores de servicios la obligación general de controlar la información que transmitan o almacenen ni la de buscar activamente indicios de actividad ilegal. Tampoco considera a los proveedores

de servicios de alojamiento de datos como responsables, en la medida en que no dispongan de un conocimiento real de la actividad o información ilegal y no tengan conocimiento de los hechos o circunstancias a partir de los cuales sea patente la actividad o información ilegal.

La Comisión ha presentado en 2018 dos nuevas propuestas: un Reglamento sobre órdenes europeas de entrega y conservación de pruebas electrónicas y una Directiva para la armonización en la designación de representantes legales para recabar pruebas en procesos penales. Las propuestas se explican en un contexto donde más del 50% de las investigaciones penales europeas incluyen una solicitud transfronteriza para la obtención de pruebas electrónicas que obran en poder de prestadores de servicios online establecidos en otro Estado miembro o externos a la UE y que debido al tiempo necesario para recabar tales pruebas o a la fragmentación del marco jurídico hace que no pueden ser debidamente investigados o enjuiciados las dos terceras partes de esas solicitudes. Además, y como subraya la Comisión, la cooperación público-privada entre proveedores y autoridades resulta ineficiente, no existe un marco legal para la cooperación voluntaria trasfronteriza, ni la adecuada certeza legal sobre el uso de pruebas electrónicas en investigaciones transfronterizas.

La Regulación obligará a todos aquellos proveedores que almacenen datos como, por ejemplo, proveedores de comunicaciones electrónicas, proveedores de hosting y similares, redes sociales, mercados on-line a consumidores finales y negocios, comunicaciones de voz o proveedores de infraestructuras de Internet. Las reglas para la solicitud de una orden de producción por un juez o fiscal desde el país de origen al proveedor del país destino dependerá del tipo o categoría de los datos asociados a la identificación del subscriptor: datos de acceso asociados al inicio y final de sesión que, por sí solos, no identifican al usuario del servicio pero que sean necesarios en las primeras fases de la investigación; datos transaccionales relacionados con la provisión del servicio o los contenidos almacenados. El proveedor deberá enviar los datos directamente a la autoridad policial del país de origen en el plazo máximo de 10 días (frente a los 120 días de media actuales), plazo que se reduce a 6 horas en situaciones excepcionales.

En paralelo, varios Estados como Reino Unido, Francia o España han revisado desde 2015 su legislación para ampliar su capacidad de interceptar individualmente -y en ocasiones masivamente- las comunicaciones en redes de telefonía e Internet o el acceso remoto a los equipos de los usuarios. El Reino Unido aprobó su Investigatory Powers Act en 2016 que permitió la obligación a proveedores de comunicaciones de mantener los registros de conexión a Internet de los usuarios (metadatos) durante un año, permitiendo el acceso remoto a ordenadores y teléfonos inteligentes para la implantación de programas de vigilancia o la descarga de información. La Ley otorgó poderes a las fuerzas de seguridad para solicitar la colaboración a los proveedores de comunicaciones para descifrar cualquier comunicación de los usuarios y consolidó la interceptación masiva de comunicaciones (metadatos). En Francia, la Loi de Renseignement y la de Mesures de surveillance des communications électroniques internationales autorizaron desde 2015 la interceptación en las redes de los operadores y el empleo de escuchas de proximidad en las redes móviles (IMSI-catchers). La legislación ampara la obtención en tiempo real de metadatos para la vigilancia individual de sospechosos y requiere a los proveedores de acceso a Internet la detección y filtrado

de patrones de tráfico potencialmente vinculados a actividades terroristas. El periodo de retención de datos varía entre 1 y 3 meses y se inicia en el instante en que se descifra la información, pudiendo retenerse para posterior análisis técnico hasta 6 años. En España, la modificación de la Ley de Enjuiciamiento Criminal de 2015 ha ampliado la obligación de colaborar con jueces y policía judicial a todos los actores que prestan un servicio on-line y permite tanto el registro remoto de equipos informáticos de uso y almacenamiento (ordenadores de usuarios y servidores en la nube).

Conclusiones

La disruptiva evolución de los servicios, redes de telecomunicaciones y tecnologías vinculadas a la Sociedad de la Información junto a la incorporación de los proveedores de aplicaciones on-line al ámbito de las comunicaciones electrónicas hace necesaria la actualización del marco legal que protege la privacidad y confidencialidad de las comunicaciones de las personas físicas y jurídicas. Con este propósito, la Comisión Europea ha propuesto a principios de 2017 el Reglamento e-Privacy, una profunda revisión de la Directiva de 2009, situando a los proveedores de aplicaciones on-line a un mismo nivel de obligaciones que los operadores de telecomunicaciones e incluyendo en la protección los terminales de usuario y las comunicaciones de datos entre máquinas (M2M/IoT).

En el mismo contexto de cambios, y para facilitar las investigaciones judiciales y policiales en su lucha contra los delitos que se cometen a través del ciberespacio, la Comisión y algunos Estados miembros han actualizado su regulación para la interceptación de las comunicaciones y obtención de pruebas. Las propuestas, elaboradas desde la primacía de la seguridad y el respaldo de la legalidad, han despertado un debate entre los reguladores y los destinatarios de la regulación. Por un lado, los distintos proveedores obligados abogan por una mayor flexibilidad, similar a la acordada para la regulación horizontal de la protección de datos, y una aplicación de la gestión de riesgo particularizada caso a caso en la protección de datos y metadatos. Por otro lado, algunos de estos desarrollos legislativos pueden tener efectos colaterales no desdeñables en materia de derechos civiles y en el ejercicio de las operaciones comerciales de empresas extranjeras, por lo que la sociedad civil exige estrictas medidas de control judicial, transparencia, legitimidad y auditabilidad a raíz de las notables capacidades técnicas de que disponen las fuerzas de seguridad para interceptar grandes volúmenes de información.

A la conciliación de intereses públicos y privados con los procesos nacionales y europeo de regulación se debe llegar mediante un proceso interactivo durante la fase de elaboración, que tenga en cuenta y permita la participación de los responsables y destinatarios, y durante la evaluación de sus resultados prácticos para permitir aprender de aciertos y errores. Una regulación que sólo tenga en cuenta los factores seguritarios, incluso en materias tan importantes como la privacidad, confidencialidad y los datos de carácter personal o el acceso a pruebas electrónicas y datos almacenados en el curso de investigaciones transfronterizas puede originar perjuicios y efectos no deseados a operadores y usuarios, contra la lógica y el derecho de la Sociedad de la Información.