LEY DE CONSERVACIÓN DE DATOS DE LAS COMUNICACIONES ELECTRÓNICAS

La información en poder de los operadores de telefonía e Internet puede ser clave.

Los datos de las comunicaciones por teléfono e Internet podrán ser solicitados para la investigación de delitos

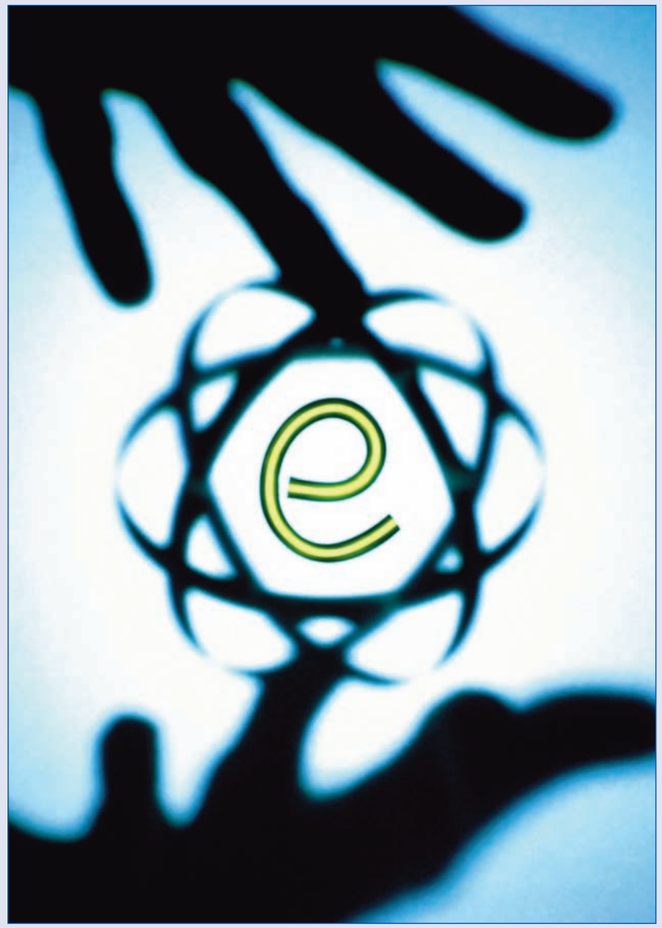
LA futura Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas, actualmente en el Senado, obligará a los operadores de telefonía fija, móvil e Internet a guardar determinados datos con el fin de favorecer la investigación de delitos. El Gobierno quiere dar un paso más a favor de la seguridad jurídica, aunque algunos sectores consideran que podría vulnerar la privacidad.

ELVIRA ARROYO

LA INVESTIGACIÓN de delitos contará en breve con nuevas informaciones que pueden aportar pistas decisivas. Con la entrada en vigor de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas, los cuerpos policiales, el Centro Nacional de Inteligencia y los funcionarios de Vigilancia Aduanera podrán acceder a una serie de datos procedentes de las comunicaciones telefónicas e Internet, que pueden ser esenciales a la hora de esclarecer sus averiguaciones.

Para ello, este proyecto de Ley –que incorpora al ordenamiento jurídico español la Directiva comunitaria 2202/58/CE– establece la obligación de que los operadores de telefonía e Internet conserven informaciones generadas durante la prestación de sus servicios. Estos datos deberán cederlos a los agentes facultados cuando los soliciten para llevar a cabo una investigación.

Los datos deberán conservarse durante doce meses, contados desde la fecha en que se produce la comunicación. Este plazo se podrá ampliar hasta un máximo de dos años o reducir a un mínimo de seis meses para determinados datos, tras consultarlo previamente con los operadores. Cuando finalice el periodo de conservación, la información se suprimirá, salvo la que se haya cedido.



Los datos deberán conservarse durante doce meses.

Privacidad cuestionada. Estas obligaciones, con las que se pretende mejorar la seguridad pública, se han implantado buscando el necesario respeto de los derechos individuales que puedan verse afectados, como son los relativos a la intimidad de las comunicaciones. En este sentido, el texto legal especifica que los datos que

‘Esta Ley pretende proteger nuestra seguridad pública en las comunicaciones y en la Red’

“LAS nuevas tecnologías han abierto posibilidades muy positivas en el mundo de las comunicaciones, pero a la vez han permitido la utilización de éstas para cometer nuevos y también viejos delitos por parte de redes de delincuencia organizada, mafias, bandas terroristas, delincuentes individuales, pederastas, etcétera. Por este motivo, es necesario que nos dotemos de los instrumentos adecuados para prevenir, investigar y dar una respuesta eficaz ante estas acciones criminales con nuevos medios técnicos, humanos y jurídicos. Eso pretende esta Ley: impedir la impunidad, garantizar el Estado de Derecho y proteger nuestra seguridad pública en las comunicaciones y en la Red.”

José Ignacio Echaniz Salgado. Diputado del Grupo Popular.

‘Los datos a retener se referirán exclusivamente a la comunicación, nunca revelarán su contenido’

“ESTA Ley transpone a nuestro ordenamiento la Directiva 2202/58/CE, que regula la obligación de los operadores de telecomunicaciones de conservar determinados datos relativos a las comunicaciones, a través de telefonía fija o móvil, con el fin de facilitarlos a los cuerpos policiales, el Centro Nacional de Inteligencia y a los funcionarios de Vigilancia Aduanera, en apoyo de sus actuaciones de investigación criminal por la comisión de delitos graves. Los datos a retener se referirán exclusivamente a la comunicación, nunca revelarán su contenido, y la cesión de datos se hará con autorización judicial previa, garantizando así el respeto de los derechos fundamentales de las personas.”

Juan Luis Rascón. Diputado del Grupo Socialista.

‘Es todo un logro que el Dictamen se aprobara en Comisión por unanimidad’

“CABE destacar que el Dictamen se aprobó en Comisión por unanimidad, lo cual en tiempos de tan abierta confrontación política es todo un logro. El proyecto trata de transponer una Directiva que establece las obligaciones de los operadores de telecomunicaciones de retener determinados datos para que puedan disponer de ellos los agentes facultados para la mejor persecución de determinados tipos delictivos. Está en juego el binomio libertad y derechos de los ciudadanos, y protección de la seguridad por parte de los poderes públicos. Equilibrar ambos valores ha estado en la base de casi todas las enmiendas, así como compatibilizar su contenido con las garantías que otorga la Ley de Protección de Datos.”

Margarita Uría Etxebarría. Diputada del Grupo Vasco EAJ-PNV.

deberán retenerse se referirán exclusivamente a la comunicación (origen y destino de una llamada o conexión a Internet; hora, fecha y duración; tipo de servicio, el equipo utilizado…) pero en ningún caso al contenido de ésta. Además, la cesión de estos contenidos exigirá una autorización judicial previa en la que se especificará la fecha límite para entregarlos.

Sin embargo, para Antoni Farriols, presidente de la Comisión de Libertades e Informática (CLI), esta iniciativa supone “no sólo una violación de la protección de datos de carácter personal, que es un derecho fundamental, sino también de la presunción de inocencia”. Ya cuando salió la Directiva Europea que ha dado lugar a esta adaptación legislativa, la CLI expresó su disconformidad ante la Comisión de Libertades del Parlamento Europeo. “La Comisión de Libertades estaba de acuerdo con nuestro planteamiento, pero pertenece al Parlamento Europeo y todos sabemos que éste tiene un peso débil dentro de la estructura política de la UE, así que la Comisión Europea aprobó el proyecto”, según Antoni Farriols.

La CLI se queja también de que, aunque la Directiva europea se refiere expresamente a que los datos almacenados deben estar disponibles para los casos de delitos graves (crimen organizado,

Los operadores que comercialicen móviles con tarjetas prepago deberán abrir un libro-registro en el que conste la identidad de los clientes

JAVIER CREMADES

Ningún usuario anónimo

ES habitual afirmar que toda actividad humana tiene sus pros y contras, su lado bueno y su lado malo. Y de tal juicio no se salvan los avances tecnológicos, internet incluido. Si la generalización de las tecnologías de la información y su uso intensivo están dotando a los individuos de medios especialmente idóneos para nuevas formas de socialización, creación de redes, acceso a la cultura, poder...; también implica –como la cruz de una moneda– singulares riesgos, como el terrorista.

El clima de inseguridad generado desde el 11 de septiembre de 2001, ha provocado que los gobiernos se hayan visto obligados a adoptar medidas legislativas que inciden en el logro de un mayor control. Estas nuevas medidas pretenden que todos los usuarios de medios como internet o la telefonía dejen un rastro con el fin de prevenir el delito o disponer de ciertas garantías de que el delincuente puede ser capturado. Para ello, resulta imprescindible evitar el anonimato con el consiguiente coste provocado por la relación inversamente proporcional que se produce entre libertad y seguridad.

> **Resulta imprescindible evitar el anonimato con el consiguiente coste provocado por la relación inversamente proporcional que se produce entre libertad y seguridad**

El pistoletazo de salida para este tipo de acciones vino de manos de los Estados Unidos a través de la promulgación, en octubre de 2001, de la denominada Patriot Act. Su preámbulo dispone la instalación de un programa espía con el fin de vigilar las comunicaciones electrónicas. Los conocidos programas Echelon y Carnivore han sido los encargados de cumplir esta función; no sin la oposición de los grupos dedicados a la defensa de los derechos civiles, dada la capacidad de vulneración de la intimidad y el secreto de las comunicaciones que estos instrumentos llevan implícita.

Europa no ha permanecido al margen de este clima de precaución. Con el fin de combatir el terrorismo y otros delitos graves, el pasado diciembre el Parlamento Europeo dio luz verde a la Directiva sobre conservación de datos generados con la prestación de servicios de comunicaciones electrónicas. La citada norma europea obliga a los operadores de telecomunicaciones a retener durante un período de seis a veinticuatro meses los datos correspondientes a números de teléfono de origen y destino, nombres y direcciones de los llamantes y llamados, así como el servicio telefónico utilizado. Además, para la telefonía móvil, se incluirá el identificador del equipo y para las comunicaciones electrónicas a través de Internet, se deberán conservar las direcciones IP, ya sean dinámicas o estáticas, los datos identificativos del abonado al que corresponda dicha IP y la datación de la comunicación. En todo caso no se podrá acceder al contenido de las comunicaciones sin previa autorización judicial. Actualmente, se está tramitando en nuestro país el proyecto de ley que adapte a nuestro ordenamiento la citada directiva.

Como es fácil suponer, con estas medidas el control y la capacidad de respuesta por parte de las fuerzas de seguridad se acentúa, pero no son eficaces al cien por cien. Muchos expertos han apuntado ya las diferentes formas por las cuales los usuarios pueden permanecer sin identificar (existen tecnologías de cifrado o enmascaramiento capaces de eludir todo rastro o confundirlo). Como bien fundamenta la exposición de motivos del proyecto de ley, las tecnologías son neutras, no son ni buenas ni malas, sino que dependen del fin para el que se utilicen. Avanzan, cambian y desaparecen a una velocidad muy superior a la que se mueve la ley, acostumbrada a regular realidades esencialmente estáticas, destinadas a permanecer. Lo que sí es cierto es que quien quiera anonimato en el uso de las nuevas tecnologías, ahora lo tiene más difícil. También lo es que conviene tutelar muy cerca el correcto ejercicio de ese poder de control, pues no puede implicar la ausencia total de libertad.

Javier Cremades es presidente del Observatorio del Notariado para la Sociedad de la Información. Autor de “Micropoder. La fuerza del ciudadano en la era digital”.

peligro de la seguridad del Estado, lucha contra el terrorismo, etcétera), en nuestro proyecto de Ley extiende la regulación a todo tipo de delitos. "Con este planteamiento, una persona que robase una naranja, sería susceptible de ser investigada", afirma Antoni Farriols. Además, "no estamos de acuerdo con el planteamiento global del tema, porque entendemos que la lucha contra el terrorismo y el crimen organizado, que todos suscribimos, está perfectamente conceptuada en la directiva 95/46 y en la ley orgánica de Protección de Datos", añade.

Tarjetas prepago. Otra novedad del nuevo texto legal es que los operadores de telefonía móvil que comercialicen móviles con tarjetas prepago deberán abrir un libro-registro en el que conste la identidad de los clientes que adquieran una línea con esta modalidad de pago. Los usuarios particulares se identificarán presentando el DNI u otro documento identificativo. Cuando el titular sea una persona jurídica, se aportará la tarjeta de identificación fiscal.

Esta inscripción será obligatoria desde la entrada en vigor de la Ley. No obstante, también habrá que realizar este trámite con las tarjetas prepago compradas con anterioridad, para lo cual los operadores dispondrán de un plazo de dos años. Una vez transcurrido este tiempo, los operadores deberán desactivar o anular aquellas tarjetas que no hayan sido anotadas en el libro-registro.

Todas estas medidas implican una adaptación tecnológica por parte de los operadores, que tendrán seis meses para poner en marcha los equipos necesarios. En opinión de la Comisión de Libertades e Informática, esto acarreará unos costes muy elevados que al final tendremos que asumir los ciudadanos. ■

Datos que deberán conservar los operadores

DATOS PARA IDENTIFICAR EL ORIGEN DE UNA COMUNICACIÓN

Telefonía móvil y fija:
- Número de teléfono desde el que se llama.
- Nombre y dirección del abonado.

Internet, correo electrónico y telefonía por Internet:
- Identificación del usuario asignada.
- Identificación del usuario y número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
- Dirección de Protocolo de Internet (IP), identificación de usuario o número de telefono asignados en el momento de la comunicación al nombre y la dirección del usuario registrado.

DATOS PARA IDENTIFICAR EL DESTINO DE UNA COMUNICACIÓN

Telefonía móvil y fija:
- Número o números marcados. En los casos en que intervengan servicios como el desvío de llamadas, los números hacia los que se transfieren las llamadas.
- Nombres y direcciones de los abonados o usuarios registrados.

Correo electrónico por Internet y telefonía por Internet:
- Usuario o número de teléfono del destinatario de una llamada telefónica por Internet.
- Nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

DATOS PARA INDENTIFICAR CUÁNDO SE PRODUJO LA COMUNICACION

Telefonía móvil y fija:
- Fecha y hora del comienzo y fin de la llamada, basadas en un determinado uso horario.

Internet, correo electrónico y telefonía por Internet:
- Fecha y hora de la conexión y desconexión a cualquiera de estos servicios, basadas en un determinado uso horario.

DATOS PARA IDENTIFICAR EL TIPO DE COMUNICACIÓN
- Servicio telefónico utilizado (fijo o móvil).
- Servicio de Internet utilizado (correo electrónico o telefonía por Internet).

DATOS PARA IDENTIFICAR EL EQUIPO DE COMUNICACIÓN DE LOS USUARIOS

Telefonía fija:
- Números de teléfono de origen y de destino.

Telefonía móvil:
- Números de teléfono de origen y de destino.
- Identidad internacional del abonado móvil (IMSI) que efectúa la llamada.
- Identidad internacional del equipo móvil (IMEI) de quien hace la llamada.
- IMSI de quien recibe la llamada.
- IMEI de quien recibe la llamada.
- Fecha y hora de la primera activación en los móviles de tarjetas prepago.

Internet, correo electrónico y telefonía por Internet:
- Número de teléfono de origen cuando se acceda mediante marcado de números.
- Línea digital de abonado (DSL) u otro elemento identificador del autor.

DATOS PARA LA LOCALIZACIÓN DE UN EQUIPO MÓVIL
- Etiqueta de localización (identificador de celda) al inicio de la comunicación.
- Datos que permiten fijar la localización geográfica de la celda.