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

www.uoc.edu/idp

Segundo Congreso sobre Internet, derecho y política: análisis y prospectiva

La conservación de los datos de tráfico en las comunicaciones electrónicas

Stefano Rodotà

Resumen

La Directiva 2006/24/CE sobre retención de datos en las comunicaciones electrónicas no es una directiva más, sino que supone un giro radical de la filosofía hasta el momento existente relativa a la protección de datos. Supone convertir de entrada a los ciudadanos en sospechosos y entrar en un nuevo marco donde se produce un fichaje masivo de datos. Esta directiva supone contravenir los principios básicos de protección de datos y también la Carta de los Derechos Fundamentales de la Unión Europea. Sin embargo, no hay que limitarse a constatar las dificultades. Existen posibilidades de hacer frente a esta nueva regulación. En primer lugar mediante la adopción de textos internacionales que regulen los derechos fundamentales en Internet (si bien el camino hacia un documento global internacional puede ser largo, no debe abandonarse). En segundo lugar, acudiendo a las instancias judiciales europeas a fin de controlar la adecuación de las disposiciones dictadas con la Carta de los Derechos Fundamentales de la Unión Europea.

Palabras clave

retención de datos, comunicaciones electrónicas, *habeas data*, privacidad

Tema

Protección de datos

Abstract

Directive 2006/24/EC on electronic communication data retention is not just another Directive, but represents a radical shift in the philosophy that has thus far existed in relation to data protection. It entails turning citizens into suspects and entering a new framework that involves large-scale record keeping. This Directive implies contravening the basic principles behind data protection, as well as the Charter of Fundamental Rights of the European Union. However, we need not limit ourselves to pointing out the difficulties. There are ways in which we can face up to this new regulation. Firstly, by adopting international texts that regulate fundamental rights on the Internet. (Even though the road towards a global international document may be long, it must not be abandoned). Secondly, by turning to European judicial proceedings in order to ensure that all regulations laid down are suitably adapted to the Charter of Fundamental Rights of the European Union.

Keywords

data retention, electronic communications, habeas data, privacy

Topic

Data protection

1. La Directiva Europea 2006/24 sobre la conservación de los datos personales no puede ser considerada simplemente como una excepción, para casos específicos y particulares, de las reglas generales de la Directiva 2002/58 sobre telecomunicaciones. Puede convertirse, y éste es el sentir de muchas personas, en una anticipación del futuro, la primera etapa hacia un cambio profundo de los principios básicos de la protección de los datos personales.

No se puede negar la necesidad de adoptar medidas adecuadas para luchar contra el terrorismo, ni la necesidad de aprovechar mejor las oportunidades ofrecidas por las tecnologías electrónicas. Pero, en un sistema democrático que se precie de serlo, esto significa en primer lugar confrontar las exigencias de seguridad y orden público con el cuadro de los derechos fundamentales. Un cuadro que hoy es más rico y complejo porque ha sido integrado con la formalización de la protección de los datos personales como derecho autónomo y fundamental, directamente conectado con la dignidad y la libertad de la persona. Y ha sido precisamente España quien primero ha reconocido esta nueva dimensión institucional incorporada en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea con una decisión del Tribunal Constitucional de noviembre del 2000, antes de la proclamación de la Carta por el Consejo Europeo en diciembre en Niza.

Mirando la realidad concreta, debemos decir que la Directiva Europea de 2006 sobre la conservación de datos generados o tratados electrónicamente cambia principios básicos de la proteción de las informaciones personales. Hay una lógica completamente distinta respecto de las directivas del pasado, un cambio en la manera de entender y regular la relación entre el ciudadano y el Estado, en la concepción misma de los derechos fundamentales de la persona. Así se reestructura no sólo el sistema jurídico sino también la organización social.

Por eso es preciso una reflexión crítica profunda. Nos enfrentamos a una alternativa que puede llegar a ser dramática y en todo caso decisiva para el futuro de la democracia. ¿Qué debemos esperar del futuro? ¿Que continúen las tendencias que han emergido con prepotencia durante los últimos años o una reactivación, aunque fatigosa, de la lógica que está en la base de la protección de los datos personales y que, con gran clarividencia, ha abierto una nueva época para la tutela de las libertades?

2. Vivimos en una época en la que la protección de los datos personales está caracterizada por fuertes contradicciones, por no decir por una verdadera y propia esquizofrenia social, política e institucional. Es cada vez mayor la toma de conciencia de su importancia no sólo para la tutela de la vida privada de las personas, sino también para su misma libertad. Sin embargo, también es cada vez más difícil respetar su naturaleza, porque exigencias de seguridad interna e internacional, intereses de los mercados, reorganización de las administraciones públicas empujan hacia una disminución de las garantías.

Para comprender el presente, y mirar al futuro, es indispensable ser conscientes del pasado. Europa ha reactivado y renovado el concepto moderno de privacidad como había sido elaborado en Estados Unidos. Conocemos los pasajes más importantes de esta historia. La autodeterminación informativa fue reconocida como derecho fundamental por parte del Bundesverfassungsgericht en 1983. En 1995, con la Directiva Europea número 46, se afirmó explícitamente que el acercamiento de las legislaciones no debía tener «por efecto un debilitamiento de la tutela por ellas asegurado, sino que al contrario, debía apuntar a garantizar un elevado grado de tutela». En el año 2000, con la Carta de los Derechos Fundamentales de la Unión Europea, la protección de los datos personales fue reconocida como derecho autónomo, contribuyendo de este modo a la «constitucionalización» de la persona, que el Preámbulo de la Carta pone «al centro» de la acción de la Unión. Y esta línea ha producido efectos institucionales importantes, como las dos comunicaciones con las que la Comisión Europea ha establecido que sus actos legislativos y reglamentarios deben estar sometidos siempre a un control preliminar de compatibilidad con la Carta de los Derechos Fundamentales. Además, siempre en el ámbito de la Unión Europea, la materia de protección de datos personales ha pasado del sector del mercado interno al de la libertad, seguridad y justicia, con un explícito reconocimiento del hecho de que nos encontramos en este momento frente a una

materia irreducible únicamente a la lógica económica, ya que toca derechos y libertades de las personas.

El marco institucional, pues, parece alentador. Pero la realidad se aleja cada vez más, y las razones de este nuevo curso son principalmente tres. Primero: después del 11 de septiembre han cambiado muchos criterios de referencia y las garantías se han reducido, como demuestran en particular la Patriot Act en Estados Unidos y las decisiones europeas sobre la transferencia a Estados Unidos de los datos de los pasajeros de las líneas aéreas y sobre la conservación de los datos personales relativos a las comunicaciones. Segundo: esta tendencia hacia la reducción de las garantías se ha extendido a sectores, como los relativos a las actividades económicas, que intentan sacar ventajas de la mutación del clima general. Tercero: las nuevas oportunidades tecnológicas ofrecen continuos y crecientes instrumentos de clasificación, selección y control de las personas, que están determinando una verdadera y propia deriva tecnológica que no siempre las mismas autoridades nacionales e internacionales contrastan adecuadamente.

Se está determinando de este modo una erosión de algunos principios sobre los que ha sido construido el sistema de la protección de los datos personales, en primer lugar el principio de finalidad y el relativo a la separación entre los datos tratados por sujetos públicos y los tratados por sujetos privados. Se tiende a imponer, incluso con forzamientos institucionales, el criterio de la multifuncionalidad. Datos recogidos para un fin determinado se ponen a disposición para fines diversos, considerados igualmente importantes respecto de los que habían justificado su recogida. Datos tratados por un sujeto son puestos a disposición de sujetos diversos.

Prevalecen las lógicas de la reutilización y de la interconexión, casi siempre justificadas con el argumento de la eficiencia y de la economicidad. Si la Administración pública conecta todos sus bancos de datos, puede dar al ciudadano servicios más rápidos, a costes más bajos y con menores molestias para los interesados. Si Magistratura y Policía pueden acceder también a las informaciones recogidas por los sujetos privados, pueden combatir mejor el terrorismo y la criminalidad. Si pueden acceder a los datos relativos a los accesos a Internet, la industria musical y la cinematográfica pueden descubrir más fácilmente quién descarga ilegalmente música y películas.

Adoptando estas lógicas, sin embargo, no sólo se contradicen principios esenciales de la protección de los datos, sino que se rompe el pacto con los ciudadanos en una materia cada vez más decisiva para la tutela efectiva de sus libertades. A ellos se les había prometido que los datos serían tratados por los sujetos públicos para finalidades específicamente individualizadas por la ley; y por los sujetos privados sólo tras el consentimiento de los interesados, que de este modo habrían podido circunscribir con precisión las utilizaciones legítimas de las informaciones recogidas.

3. La nueva directiva es uno de los ejemplos más claros de este cambio de la lógica fundamentadora de la protección de los datos personales, que corre el riesgo de convertirse en el cuadro normativo del futuro. No se trata sólo de una invasión de la esfera privada de los particulares. Las nueva reglas están reestructurando el espacio «interior» y «exterior» del ciudadano, con referencia a una situación específica, pero con un planteamiento que puede difundirse a otras materias, llegando a una progresiva marginación de la elección que desde la Directiva 95/46 y las especificaciones contenidas en la Directiva 2002/58 se ha producido, y del artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea que ha reconocido la protección de los datos como un derecho fundamental, autónomo y distinto de la tutela tradicional de la vida privada y familiar.

En la última directiva pueden notarse tres tendencias convergentes y todas ellas restrictivas de la intensidad de la protección de los datos: tendencias hacia la totalidad, la permanencia y la disponibilidad de las informaciones recogidas. Sus normas ilustran bien las cuestiones de la totalidad (conservación del conjunto de todos los datos relativos a las comunicaciones electrónicas), de la permanencia (de seis meses a dos años, pero con la posibilidad para los Estados miembros de superar estos plazos de tiempo), de la disponibilidad total (referencia genérica a «delitos graves», desde el punto de vista objetivo, a «autoridades nacionales competentes» desde el punto de vista subjetivo). En los dos casos faltan especificaciones que podrían limitar una peligrosa discrecionalidad, que no puede admitirse cuando hablamos de derechos fundamentales.

Es de este modo evidente como se dan la erosión, o el abandono, de principios básicos de la protección de datos personales –finalidad, proporcionalidad, pertinencia y necesidad. En la Directiva 2002/58, la conservación de los datos de tráfico se limita al tiempo necesario para la facturación. Ahora, la relación entre la recogida de los datos y la finalidad comercial está borrada, se impone una finalidad distinta y ulterior, la eliminación de la separación entre los datos tratados por sujetos públicos y los tratados por sujetos privados. Se tiende a imponer el criterio de la multifuncionalidad. Datos tratados por un sujeto son puestos a disposición de sujetos diversos.

Una confirmación muy significativa del abandono de estos principios se ha recibido de la Administración americana, que ha pedido a Google datos, incluso agregados, sobre los accesos a determinados sitios con el argumento de la lucha contra la pedofilia. La lógica de esta petición es muy clara: irrelevancia de las finalidades para las cuales ha sido constituido un banco de datos; consiguiente disponibilidad de los datos para cualquier utilización que se considere importante para el alcance de un interés público y cancelación del confín entre bancos de datos públicos y privados. Se manifiesta una nueva dimensión de la vigilancia, que exalta el poder del Estado para disponer de cualquier información personal, recogida por cualquiera e independientemente de las finalidades originarias de la recogida. El conjunto de los datos tratados por los privados está considerado como un recurso a disposición de los poderes públicos.

La lógica que se manifiesta en la Directiva sobre la conservación de los datos es la misma. Se afirma un poder absoluto del Estado de poner las manos sobre el «cuerpo electrónico» de los ciudadanos, frente al que se debe reaccionar reivindicando con fuerza un *habeas data* capaz de atribuir al cuerpo electrónico la protección que el *habeas corpus*, hace ochocientos años, dio al cuerpo físico, reaccionando a las pretensiones absolutistas del rey. La constitucionalización de la persona, visible al menos en el sistema de la Unión Europea, impone que nos movamos en esta dirección.

4. La ruptura del esquema fundado en el principio de finalidad y en la fuerza del consenso es también el efecto de una tendencia más general hacia la extensión de la recogida de información a un número cada vez mayor de personas. Se pasa de la recogida con miras a la recogida generalizada. Se amplía el área de las personas sometidas a control. Ya no sólo personas solas o grupos considerados peligrosos: en este momento la población entera está considerada como «una potencial clase peligrosa» (y también, en otros casos, como un único conjunto de consumidores) que justifica la creación de recogida «total» de datos y la incesante producción de perfiles individuales, familiares, de grupo, basados en informaciones que atañen también a la salud, a la situación financiera y a las elecciones culturales.

Esta recogida de datos personales a escala de masa ya ha determinado la transformación de todos los ciudadanos en potenciales sospechosos, frente a los poderes públicos, y la objetivación de la persona, frente al sistema de las empresas. Además, la creciente posibilidad por parte de sujetos públicos de interconectar todos sus bancos de datos y de obtener información de cualquier fuente privada produce una transparencia social sin precedentes, que cambia la posición del ciudadano en las sociedades democráticas y su relación con el Estado.

La Directiva crea así «naciones de sospechosos». La multitud ya no es más «solitaria», como la describía en los años cincuenta el sociólogo americano David Riesman. Está ahora ya «desnuda», continuamente escrutada a través de las diversas tecnologías. Y la manera como está estructurada la Directiva manifiesta claramente que no nos enfrentamos a una situación transitoria: aquí el oxímoron «emergencia permanente» manifiesta toda su potencia y la regla «excepcional» se constituye como verdadera y estable disciplina del futuro.

Esta nueva construcción social determina una situación en la cual es previsible que la existencia de enormes bancos de datos produzca presiones hacia una multifuncionalidad más y más amplia. Ya la industria musical y la cinematográfica piden acceso a los datos relativos a Internet para descubrir más fácilmente quién descarga ilegalmente música y películas.

Frente a esta situación concreta, el *considerando* 17 de la Directiva no es sólo la manifestación de una contradicción, o una verdadera paradoja, porque se dice que «la presente Directiva intenta garantizar el pleno cumplimiento de los derechos fundamentales del ciudadano, el respeto de la vida privada y de las comunicaciones y la protección de los datos de carácter personal, consagrados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea». Es la señal de una incapacidad política e institucional de comprender qué significa hoy la dimensión de la libertad y de los derechos en la dimensión del cyberspace. No se hace ninguna ponderación entre la necesidad de la lucha contra el terrorismo y el conjunto de los derechos fundamentales; no se hace ninguna evaluación de las nuevas medidas en la perspectiva de los principios de finalidad, proporcionalidad, pertinencia y necesidad.

El efecto es el abandono del criterio del «alto nivel de protección», indicado en la Directiva 95/46. Ninguna indicación del Parlamento Europeo, del Consejo Económico y Social, del Grupo de Trabajo del art. 29 y del Supervisor Europeo ha sido aceptada en relación con la especificación de las categorías de datos recogidos, de «delitos graves», de los sujetos que pueden acceder a los datos. Las garantías son inadecuadas, empezando por la que quería ser la más significativa y que atañe a la exclusión de los datos relativos a los contenidos de las comunicaciones, que ha sido presentada como un éxito importante de la discusión sobre el tema.

Un ejemplo extraído de la experiencia italiana puede ayudarnos a aclarar la dimensión del problema. Cada día en Italia se hacen 800 millones de llamadas telefónicas y se envían 300 millones de correos electrónicos. El total, en un año, es de casi 400.000 millardos de comunicaciones electrónicas. Puesto que los datos se conservan por lo menos durante cuatro años (pero se puede llegar a seis), esto significa que los bancos de datos de los gestores de las comunicaciones contienen al menos un millón seiscientos mil millardos de datos personales. Incluso sólo la conservación de las direcciones del remitente y del destinatario permite reconstruir la trama de las relaciones personales y sociales (¿cuántas veces he llamado a una determinada persona?), políticas y sindicales (¿con qué organizaciones estoy en contacto?), económicas (¿cuáles son las empresas, los agentes de bolsa con los que mantengo relaciones?), concernientes a la fe religiosa (¿mi

interlocutor es la parroquia, la sinagoga, la mezquita?). Aún más delicada, si cabe, es la conservación de los datos que atañen a los accesos a los sitios Internet, debido a la mayor elocuencia de estos accesos respecto a gustos, preferencias, inclinaciones. ¿Podemos aceptar este fichaje de masa? ¿Hay proporción entre el fin indicado y el instrumento utilizado? ¿Podemos aceptar la transformación de los ciudadanos en «networked persons», personas continuamente controladas electrónicamente en su vida ordinaria? Frente a estos datos, no es posible afirmar que el principio de proporcionalidad sea respetado.

Y la ausente conservación de los contenidos de las comunicaciones corre el peligro de volverse un boomerang, no una garantía. Si he hecho una llamada telefónica inocente a quien luego se revela un criminal, la imposibilidad de demostrar cuál ha sido el verdadero contenido de la comunicación dejará sobre mí la sombra de la sospecha. Una sospecha que incluso puede ser construida: visto que deben registrarse también los intentos de llamada no conseguidos, alguien podría llamarme en un momento en el que sabe que no me encuentro en condiciones de contestar, creando así la apariencia de una relación que me une a esa persona, que yo podría incluso no conocer.

Nos enfrentamos aquí a una situación en la cual no hay sólo una erosión de los principio básicos de la protección de los datos, sino de uno de los principios básicos de la civilización jurídica, la presunción de inocencia.

Estas nuevas, gigantescas recogidas de informaciones, además, pueden revelarse inefectivas y hacen aumentar la vulnerabilidad social. En un documento de trabajo del Parlamento Europeo, realizado por el diputado Alexander Nuno Alvaro, se recuerda que la red de un gran proveedor de Internet con las nuevas normas tiene que recoger una cantidad de datos similar a 20-40.000 terabyte, con la consecuencia de que, con las tecnologías actuales, la búsqueda podría durar hasta 50 años. Y además cada uno de nosotros se expone al riesgo de que los propios datos vayan a parar a manos de quien consigue entrar ilegalmente en estos enormes y no siempre demasiado seguros bancos de datos y que informaciones delicadas sean puestas en circulación por empleados infieles de las empresas que tienen la gestión de la recogida de información. Es un riesgo concreto. El año pasado se robaron los datos de 52 millones de clientes de Mastercard, y el Senado de Estados Unidos, consciente de estos peligros, ha aprobado una propuesta de ley que obliga a los gestores de los bancos de datos a informar a sus clientes de los peligros de «robos de identidad». Cambia la naturaleza de la protección de los datos, y con ella cambia la entera organización social.

No estamos discutiendo una directiva sectorial. Nos enfrentamos a una verdadera redistribución de poder social, una redefinicion de la posición de la persona y de la ciudadanía. El ataque del terrorismo es grande y debe ser rechazado. Sin embargo, en esta lucha la democracia no puede perder su verdadera y profunda naturaleza, que es históricamente su arma más fuerte para contrastar cualquier ataque.

5. Sin embargo, en ésta y en otras materias, no podemos limitarnos a constatar las dificultades, a buscar sólo alguna «estrategia de cazador furtivo» o incluso a resignarnos a la impotencia. Es posible, en cambio, indicar algunas estrategias posibles.

La primera atañe, obviamente, a iniciativas que tienden a ampliar el espacio de reglas comunes que tienen precisamente en la Unión Europea su lugar más significativo. Desde el año 2000, con la Carta de Venecia, las autoridades para la protección de los datos personales han indicado la vía de una convención internacional, idea que fue tomada en consideración nuevamente en la última conferencia de Montreux. El pasado mes de noviembre, en el

World Forum on Information Society, organizado en Túnez por la ONU, se habló de una Carta de los Derechos para Internet. Esta hipótesis fue sometida en enero del 2006 a la Comisión de Libertades Públicas del Parlamento Europeo. En Estados Unidos se presentó a la Cámara de los Representantes, en mayo del 2005, un Global Internet Freedom Act, y la petición de reglas internacionales de tutela de la libertad de expresión se hizo más fuerte tras los recientes episodios de censura que vieron como protagonistas a Microsoft y Yahoo, por lo que se refiere a China, y que alarmaron también a Reporters sans Frontières. El camino hacia un documento global internacional es seguramente largo. Pero no debe abandonarse. Mientras, es necesario seguir con atención lo que ocurre en el área de MERCOSUR y es posible empezar a tomar iniciativas sobre temas específicos, dialogando por ejemplo con Estados Unidos sobre el tema del *spamming*, tal y como había empezado a hacer la pasada Comisión Europea, o sobre las nanotecnologías, tal y como sugiere la Cnil.

Es necesario retomar pues la línea adoptada por el Parlamento Europeo, que ha impugnado ante la Corte de Justicia la disposición relativa a la transferencia a Estados Unidos de los datos de los pasajeros de las líneas aéreas. Se debe empezar a tomar en consideración la impugnación de disposiciones nacionales que aplican decisiones de la Comisión que violan los derechos fundamentales de los ciudadanos. Pero es también necesario tomar en serio lo que la Comisión ha dispuesto a propósito de la necesidad de control de conformidad a la Carta de los Derechos Fundamentales de la Unión Europea, que de otra manera corre el peligro de reducirse a una cláusula de estilo. En el considerando 22 de la Directiva sobre la conservación de los datos, por ejemplo, con una argumentación paradójica se afirma que la restricción de la libertad de comunicación garantiza mejor precisamente los derechos previstos por los artículos 7 y 8 de la Carta. Ha llegado el momento de empezar a pedir a la Corte de Justicia que controle la validez del modo como se efectúa la declaración, de conformidad a la Carta, en los actos de la Comisión.

Más en general, con todos los medios disponibles y aprovechando todas las oportunidades, es urgente frenar la contaminación creciente del ambiente de las libertades civiles producida por el conjunto de normas que, con varias motivaciones, restringen la protección de los datos personales. Esto es indispensable para evitar que el recurso a las innovaciones científicas y tecnológicas favorezca la consolidación de una sociedad de control, de clasificación y de selección social. Y esto es necesario también para dar a las innovaciones tecnológicas esa legitimación social que hace nacer la confianza de los ciudadanos, haciendo posible así un mejor funcionamiento de la *business community*.

Esta labor está haciéndose cada vez más difícil, y a menudo nos preguntamos si realmente la protección de los datos personales puede sobrevivir con las esperanzas y las expectativas con las que se había creado. Sin embargo, como ha escrito Spiros Simitis, sigue siendo «una utopía necesaria». Una utopía, sin embargo, que no dirige nuestra mirada hacia un futuro lejano, sino que la obliga a considerar la realidad que está a nuestro alrededor. La protección de los datos personales es ahora ya una dimensión de la libertad de los contemporáneos. No es retórica recordarlo en cada ocasión, porque cada una de sus variaciones incide sobre la medida de democracia de la que cada uno de nosotros puede gozar.

Cita recomendada

RODOTÀ, Stefano (2006). «La conservación de los datos de tráfico en las comunicaciones electrónicas». En: «Segundo Congreso sobre Internet, derecho y política: análisis y prospectiva» [monográfico en línea]. *IDP. Revista de Internet, Derecho y Política.* N.º 3. UOC. [Fecha de consulta: dd/mm/aa].
<http://www.uoc.edu/idp/3/dt/esp/rodota.pdf>
ISSN 1699-8154

Stefano Rodotà

Expresidente de la autoridad italiana garante de la protección de los datos personales y expresidente del Grupo del Artículo 29 sobre protección de datos de la Unión Europea.