

**Voces:** TELECOMUNICACIONES ~ INTERNET ~ CORREO ELECTRONICO ~ INFORMATICA

**Título:** La controversia sobre la retención de datos de tráfico en Internet

**Autor:** Palazzi, Pablo A.

**Publicado en:** LA LEY 28/04/2005, 28/04/2005, 1

Una gran confusión se ha generado en torno a la ley que obliga a almacenar datos de tráfico en materia de telecomunicaciones. Primero, varios artículos periodísticos sostuvieron que la reglamentación permitiría espiar el correo electrónico y vigilar a quienes navegan por Internet en violación a su privacidad. Asimismo, la cámara que nuclea a empresas de telecomunicaciones inició un amparo en contra de la aplicación del decreto, con fundamento en los costos que acarrea el cumplimiento de la medida. Los legisladores, frente a estas noticias, dijeron que el error había sido del Poder Ejecutivo al reglamentar la ley. El presidente de la Nación, -desde Alemania-, aseguró que derogaría la norma que él mismo había aprobado unos meses antes.

La ley 25.873 (Adla, LXIV-A, 151) reguló tres aspectos diferentes de la cuestión: (i) la obligación de toda empresa de telecomunicaciones de colaborar con una investigación en la justicia y en concreto con los pedidos de informes (que se trata de una carga pública como la de ser testigo o jurado); (ii) la obligación de retener ciertos datos de tráfico en materia de comunicaciones (telefónicas, por Internet y por cualquier otro medio novedoso como la telefonía IP) por el plazo de 10 años y (iii) la responsabilidad estatal por los daños que esta actividad pueda ocasionar.

La ley tiene varios aspectos criticables. Estos son: el excesivo plazo de una década para almacenar la información (que en el derecho comparado no supera los 2 ó 3 años) y los costos a cargo de las empresas de telecomunicaciones. Esto hace a la ley imposible de cumplir económicamente, sobre todo para las empresas más pequeñas. A ello se suma el breve plazo previsto en el decreto reglamentario para su entrada en vigencia, transformando lo que es una carga pública (el deber de colaborar con la justicia) en una cuasi-expropiación. En este aspecto, la ley podría ser inconstitucional, no por afectar el derecho a la privacidad sino porque violaría el derecho de propiedad de las empresas. Una futura reforma debería acortar los plazos y revisar la distribución de los costos en forma razonable. Cabe agregar que estos cambios en modo alguno afectarían el balance que se buscó con la norma: poder investigar el delito y evitar que la tecnología, sobre todo la desarrollada por el sector privado, se transforme en un obstáculo para que la justicia cumpla con sus cometidos.

Después está el tema de la privacidad. El hecho de almacenar datos de tráfico

en materia de telecomunicaciones puede generar temor en más de alguno. El lector no se confundirá si se siente vigilado con este almacenamiento de las direcciones de sitios de Internet a los que accede, las personas a las que envía email, o la ubicación geográfica del equipo desde donde "chateó" por última vez. En el siglo XVIII Jeremy Bentham, en su obra El Panóptico, describía un método muy similar, aunque más rudimentario, para vigilar prisiones (cuyo fundamento último era hacer que los individuos actuaran en cierta forma si se sentían observados). Para evitar esto, la gente podrá recurrir a tecnología que permita el anonimato, o usar métodos de encriptado. Este almacenamiento de datos en muchos casos ya tenía lugar desde hace tiempo y nunca nadie protestó por ello. Por ejemplo, las empresas telefónicas tienen que almacenar los datos relativos a nuestras llamadas para poder facturarlas. El correo oficial se queda con información de envío de correspondencia postal y lo mismo hacen los correos privados. Esta es información sobre el tráfico de la comunicación, no sobre el contenido.

Pero ni la ley ni el decreto cuestionados permiten que esta "vigilancia" tenga lugar sin control. Para llegar a dicha conclusión basta leer detenidamente el texto de ambas normas. Lo que establece la ley es que el almacenamiento será sólo de datos de tráfico, esto es, de la información asociada a una comunicación que expresa el emisor, el destinatario y otros elementos como la hora del envío y la ubicación geográfica del creador del mensaje. No cabe ninguna duda que esta información es de gran utilidad para cualquier investigación judicial. Pero esta información no equivale al contenido del mensaje. Por ende ni la ley ni el decreto obligan a guardar el contenido de correos electrónicos, ni el de "chats" o las conversaciones realizadas a través de los programas de mensajería instantánea. Estos contenidos sólo son almacenados en forma temporaria por las empresas, pero no se les aplica el plazo de 10 años (por eso el decreto habla de monitoreo u observación "en tiempo real" para esta clase de datos en el art. 2). La obligación de guardar por una década se aplica entonces sólo a los datos de tráfico y de clientes (por eso el art. 3 del decreto habla de "acceso" y de "conservar").

Hay sin embargo un punto donde los datos de tráfico y los de contenido se juntan y esto tiene lugar cuando se realiza un "log" de los sitios web recorridos por un internauta, pero como explicamos seguidamente, el acceso a esta información está a buen resguardo con la previa intervención judicial.

De conformidad con nuestro sistema constitucional, tanto para acceder al contenido de una comunicación como para acceder a la información asociada a ella se requiere orden de juez competente. Esto surge del art. 18 de la Constitución ("... es inviolable ... la correspondencia epistolar y los papeles privados ..."), y de los arts. 5, 21 y 22 de la ley 25.520 de inteligencia nacional

(Adla, LXII.A, 22). Esta ley constituyó un gran avance, pues a la par de regular en forma integral los servicios de inteligencia (con límites muy sanos), expresamente se aclara en su art. 5 que toda clase de comunicación -telefónica, por Internet, y por cualquier otro medio- está amparada por la privacidad y sólo con orden de juez competente se podrá proceder a su interceptación. Esta interpretación se refuerza, porque la ley de datos de tráfico (ley 25.873, arts. 1° y 2°) requiere expresamente que la colaboración de las empresas de telecomunicaciones y la sistematización de datos de tráfico tenga lugar "de conformidad con la legislación vigente". Por último, el Código Procesal Penal requiere para incautar estos datos una orden fundada de juez (art. 236 CPP), salvo las reformas de la ley 25.760 respecto de las facultades fiscales en casos de secuestros).

La única forma de obtener el contenido de una comunicación digital es entonces con una orden judicial. Toda otra interpretación sería inconstitucional. Además los registrados en esas bases de datos de empresas de telecomunicaciones tienen derecho a acceder a esta información y conocer que se sabe de ellos, en virtud de la garantía constitucional de hábeas data (art. 43, Constitución Nacional).

El sistema implementado por la ley es de gran utilidad en las investigaciones de delitos virtuales. También es de utilidad en juicios de derecho privado, donde se discuten injurias o calumnias por Internet, robo de información confidencial o secretos comerciales. La información de datos de tráfico permite reconstruir lo que ha ocurrido en el mundo virtual y a largo plazo encontrar y juzgar a responsables de hechos ilícitos.

Ahora, si la norma se deroga debido a toda la confusión reinante, habremos perdido una importante herramienta legal para combatir el delito cibernético que esta vigente en Europa y Estados Unidos. Si en el pasado han existido abusos por parte de los "servicios" en esta materia, que derivaron en claras violaciones a la privacidad, el mal no se combate quitándole estas herramientas, sino sancionando a los culpables de estos hechos.