El laberinto de la identificación en internet

Enviado por marta el Mar, 11/20/2012 - 11:52
Antetítulo (dentro):
CRIMINALIZACIÓN EN LA RED | Muchos juzgados emiten requerimientos de datos personales fuera de las garantías
Sección principal:
Saberes
Cuerpo:

A principios de octubre, la filtración del sumario que instruía la Audiencia Nacional para juzgar a los supuestos organizadores de las protestas del 25S alrededor del Congreso puso el acento sobre el acceso a los datos de internautas por parte de instituciones judiciales. A la mayoría de las personas nombradas en el sumario se les identificó por observación policial en asambleas, pero algunas figuraban porque gestionaban las cuentas de “Ocupa el Congreso” en Facebook y Gmail. Para llegar hasta ellas, la Brigada de Investigación Tecnológica de la Policía Nacional tuvo que solicitar su identidad a estas compañías.

La Ley de Servicios de la Sociedad de la Información y de comercio electrónico (LSSI, de 2002) obliga a todos los proveedores a guardar los logs –registros de actividad– durante un año. Deben preservar fecha y hora de inicio y fin de la comunicación con el servidor donde estén alojados los datos y el número IP que identifica el punto desde el que se hace la petición (es decir, el ordenador con el que me conecto para consultar mis mensajes, por ejemplo). También la Ley de Protección de Datos establece que las instituciones judiciales pueden ordenar a las prestadoras de servicios la cesión de datos e, incluso, el contenido de las comunicaciones de los usuarios. Pero las grandes empresas de la web suelen quedar fuera de estas legislaciones y responden a los requerimientos según su propio parecer, aunque atadas al Tratado de Auxilio Judicial en Materia Penal entre los EE UU y España y al Acuerdo de Asistencia Judicial entre la Unión Europea y EE UU.

Según explica un documento del Consejo General del Poder Judicial (CGPJ) publicado en su web, en muchos casos los tribunales españoles se saltan la ardua burocracia de pasar la comisión rogatoria al Departamento de Justicia estadounidense para conseguir información relacionada con logs. “Basta expedir un mandamiento judicial a la empresa que concrete correctamente la denominación de la cuenta de correo, URL, etc. e indicar expresamente los datos que de los mismos se soliciten”, explica el documento.

La privacidad va por barrios

Algunas plataformas lo dan más mascadito. Microsoft, que presta los servicios de Hotmail, MSN y Windows Live, gestiona las peticiones de los juzgados a través del departamento legal de su oficina en Madrid, Microsoft Ibérica, y proporciona a las instituciones los datos que estipula la LSSI. Facebook también ha hecho lo que estaba en su mano para facilitar el trabajo de investigación: según explica en una pequeña guía sobre cómo pedir información sobre sus usuarios, la compañía tiene un departamento destinado a atender las peticiones de los juzgados, a los que facilita vía mail o por servicio postal información de registro y las IP desde las que el usuario ha accedido a su cuenta en los 90 días anteriores a la solicitud. Eso sí, reservándose el derecho de “aplicar tarifas razonables para cubrir los costes”.

Otras empresas tienen más reparos y hacen gala de proteger a sus usuarios cumpliendo escrupulosamente las garantías judiciales. Twitter y Google (del que depende Gmail) publican informes sobre las peticiones de información que reciben por parte de gobiernos. La primera ha recibido por parte de instituciones judiciales españolas desde enero hasta junio menos de diez solicitudes en relación a doce usuarios, de las que no ha respondido a ninguna; la segunda recibió de julio a diciembre de 2011 hasta 388 referentes a los datos de 610 usuarios, de las que respondió poco más de la mitad. El resto fueron rechazadas por defectos de forma, o bien se les pidieron datos que no tenían.

El tema se complica cuando lo que se quiere es conocer el contenido. “El contenido de las comunicaciones sí está claro que sólo puede pedirse mediante un auto judicial motivado”, explica el abogado Carlos Sánchez Almeida, especializado en tecnología. La Ley de Enjuiciamiento Criminal señala que el juez puede ordenar la intercepción de las comunicaciones de un sospechoso durante un plazo de tres meses. En el caso de prestadoras de servicios de EE UU, el juez no puede ya esquivar la comisión rogatoria a su Departamento de Justicia, solicitando antes directamente a la compañía la conservación de los datos a través de la Brigada de Investigación de Delitos Tecnológicos. En raras ocasiones dan respuesta si no es en relación a delitos muy graves, como homicidio o atentado terrorista. El documento del CGPJ explica que más lejos aún queda la intercepción en tiempo real, posible sólo “si en dicha investigación pudiese intervenir el FBI”.

Durante la investigación sobre el 25S, Facebook y Google sólo facilitaron las IP desde las que se gestionaron las cuentas. Con ellas en su poder, la Policía tuvo que dirigirse a las operadoras de conexión a internet: Vodafone, Jazztel Telecom, R Cable y Telecomunicaciones de Galicia, Telefónica y Orange. Éstas no practican ningún mecanismo de transparencia y no se sabe cuántas peticiones reciben ni cómo responden.

Legislación ‘dinámica’

La Ley 25/2007, de conservación de datos relativos a las comunicaciones electrónicas nació para regularizar y estandarizar el proceso. El problema es que parece haber quedado en papel mojado: en su primer artículo, la ley establece la obligación de los operadores de ceder los datos de los usuarios requeridos por autorización judicial para la investigación, detección y enjuiciamiento de delitos graves, que tienen una pena de prisión mínima de cinco años. Sin embargo, según Sánchez Almeida, “este tipo de datos se está pidiendo de forma indiscriminada”.

En la práctica, la mayoría de los juzgados aplican en este tema la doctrina del Tribunal Constitucional, que dejaba la decisión a criterio de los jueces, o acuden a otras normas, como la Directiva 2005/60/CE del Parlamento Europeo sobre blanqueo de capitales y financiación del terrorismo, que interpreta como delitos graves aquellos con una pena superior al año de prisión. Sólo la Audiencia Provincial de Barcelona parece acordarse de la ley aprobada en 2007, señalando por primera vez en una resolución que los datos recogidos por un operador de telecomunicaciones no pueden ser reclamados en relación a un delito no grave.

Y el dilema final viene al calibrar el peso de una dirección IP como prueba judicial. “Hemos conseguido sentencias absolutorias porque no se podía saber a ciencia cierta quien había usado la terminal”, comenta Sánchez Almeida. Las direcciones IP, aunque se correspondan con dispositivos cuyo dueño esté identificado, tienen poco peso por sí solas a la hora de condenar a alguien porque se puede acceder a conexiones ajenas a través de wi-fi.Las IP dinámicas complican aún más el asunto. “Hacen falta más factores”, concluye el abogado.

Falta conocer los detalles de la reforma del Código Penal para ver si introducirá elementos para perseguir a quienes convocan acciones por internet, aunque el acceso a datos personales por parte de la Policía seguirá quedando a discreción de quien los administre mientras no cambie la directiva europea que marca que los servidores están sujetos a la jurisdicción del lugar donde se encuentran –está previsto, pero no para antes de 2015– o las proveedoras de conexión apliquen criterios más transparentes.

EL CASO DE LOS SERVIDORES AUTOGESTIONADOS

Los movimientos sociales han tratado de dotarse de su propia infraestructura de servidores autogestionados para, entre otros motivos, escapar al control que puede ejercer la Policía. “Nosotros siempre vamos a requerir que toda petición de datos sea hecha expresamente por un juez”, cuenta Roxu, de Sindominio.net, que opina que “el problema no va a venir tanto por los jueces, sino por los proveedores y grandes empresas”.

Para empezar, si quien administra un servidor no tiene ánimo de lucro, la Ley de Servicios de la Sociedad de Información no le afecta igual que a las empresas y no es obligatorio que guarde los registros de actividad durante tanto tiempo. Además, puede configurar mecanismos para hacer técnicamente imposible las identificaciones, por ejemplo montar un CDN –red de distribución de contenidos por sus siglas en inglés– en el que las IP se sirvan desde distintos puntos que no se puedan trazar.

Otra opción es escapar de las leyes estatales y optar por alojar los datos en países con legislaciones más garantistas. Así lo han hecho Nodo50 y el colectivo Lorea, que mantiene la red social N-1.cc. Ambos contrataron sus servidores a iPredator, una pequeña empresa situada en Suecia y vinculada al colectivo The Pirate Bay, especialista en blindarse ante demandas de censura de contenidos por motivos de copyright.

A medida que los movimientos sociales hacen un uso más intensivo de las redes comerciales, se va descuidando la seguridad. Cuando se extendieron las acampadas del 15M, la comisión Hacksol decidió contratar los servidores para los blogs y las listas de correo de Tomalaplaza.net a la multinacional francesa OVH.

Esta compañía es apreciada porque alojaba la web de Wikileaks y resistió a las presiones de EE UU y Francia en pleno escándalo de los cables diplomáticos, negándose a borrar nada sin una orden judicial que finalmente no llegó. Sin embargo, que la administración de los servidores la haga una empresa opaca siempre limita la certidumbre acerca de quién está accediendo a ellos. “Por eso es importante que tengamos recursos autogestionados, que dependan de comunidades de afines”, concluye Roxu.

Temáticos:
Número 184
Edición impresa:

Posición Media:
Columna derecha
Compartir:

Tipo Artículo:
Normal
Autoría foto:
Olmo Calvo
Info de la autoria:
Redacción
Autoría:
Ter García
Marta G. Franco