

ANTONIO TRONCOSO. DTOR. DE LA AGENCIA DE PROTECCIÓN DE DATOS DE MADRID

'El Constitucional debió admitir a trámite el recurso contra Sitel'

La Agencia Española de Protección de Datos investiga si el Sistema Integral de Interceptación de las Comunicaciones Electrónicas (Sitel) cumple con la legalidad. La directora de la Agencia de Protección de Datos de Cataluña, Esther Mitjans, dijo a LA GACETA que el software es "claramente ilegal e inconstitucional". Ahora habla su homólogo madrileño, Antonio Troncoso, quien cree que el Tribunal Constitucional debería haber enjuiciado el sistema cuando la Asociación de Internautas se lo pidió.

[Roberto R. Ballesteros. LA Gaceta.-](#) - ¿Por qué piensa así ?

No es razonable que el Constitucional no admita a trámite el recurso de amparo por no encontrar suficientemente justificada "la trascendencia constitucional" del mismo.

-¿Por qué?

-Teniendo en cuenta la jurisprudencia del propio Constitucional y del Tribunal Europeo de Derechos Humanos, está claro que un recurso, especialmente en relación con la conculcación del secreto de las comunicaciones antes de la Ley de 25/2007, tiene trascendencia constitucional. Cuando hablamos de conversaciones políticas, el secreto de las comunicaciones es garantía no sólo de la intimidad, sino de la propia democracia. El control del poder no se consigue limitando el secreto de las comunicaciones -por ejemplo, de políticos-, sino con mayor acceso a información administrativa.

No se controla con escuchas, sino con más transparencia''

-¿Qué información está protegida por el secreto de las comunicaciones?

-La jurisprudencia ha reconocido que la protección se extiende no sólo al contenido de la conversación, sino a la identidad subjetiva de los interlocutores. Por tanto, el acceso por parte de la Policía a los números marcados requiere intervención judicial, tanto para su autorización como para el control de su ejecución. El Tribunal Europeo de Derechos Humanos, en 1981 (caso Malone), condenó al Reino Unido por incluir en los eugimientos realizados al señor Malone un sistema que informaba automáticamente sobre cuáles eran los números de teléfono a los que llamaba. Asimismo, la sentencia 114/1984 del TC incluía dentro del secreto, "no sólo el contenido de la comunicación, sino también otros aspectos como la identidad subjetiva de los interlocutores".

-¿Cree suficiente la cobertura legal que ampara Sitel

-Hasta la Ley 25/2007 no había una regulación adecuada. Es complejo determinar si algunos preceptos de esta norma deberían tener el rango de ley orgánica. Sí creo que las fuerzas de seguridad deben disponer de una legislación clara que dé seguridad jurídica a su actuación y que asegure que la ejecución de la orden judicial respeta el principio de proporcionalidad.

-¿En qué afecta Sitel a la protección de datos?

-Una empresa de comunicaciones está obligada por la ley a dar a la Policía toda la información sobre la identificación de la persona, su domicilio, el número de titularidad del servicio, el número de cuenta asignada al proveedor de Internet, la dirección de correo electrónico, la situación geográfica del terminal y otros datos sin orden judicial. Es legítima por lo tanto la comunicación de datos personales a la Policía, sin consentimiento del interesado, siempre que resulten necesarios para la prevención de un peligro real y grave para la seguridad pública o para la represión de infracciones penales. Esta comunicación está habilitada por la Ley Orgánica de Protección de Datos y por la legislación de Fuerzas y Cuerpos de Seguridad del Estado.

Cómo debe ser la petición?

-Concreta y específica. Debe quedar constancia de ella, estar motivada y realizada por una persona con autoridad, de forma que se acredite que la petición de datos personales es necesaria para la prevención o para la persecución de las infracciones penales. La legislación de protección de datos obliga a implantar en los ficheros policiales -también en los utilizados para la interceptación de las comunicaciones medidas de seguridad de nivel alto -cifrado, registro de accesos-, que garantizan que las transcripciones no sufren modificaciones y que sólo acceden a ellas las personas que llevan a cabo las investigaciones, no los cargos políticos. Esto es especialmente importante cuando el sumario ha sido declarado secreto. La misma normativa obliga a cancelar los datos personales registrados con fines policiales cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento. Esto tiene relevancia porque las transcripciones de conversaciones afectan a la intimidad.

Saber más sobre la Interceptación de las Comunicaciones en España

Fecha artículo: 2010-01-16 16:48:31 - url artículo: <http://www.internautas.org/html/5949.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2010 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org