

**GRUPO PARLAMENTARIO POPULAR
EN EL CONGRESO**



A LA MESA DEL CONGRESO DE LOS DIPUTADOS

El Grupo Parlamentario Popular en el Congreso, al amparo de lo dispuesto en el artículo 193 y ss. del vigente Reglamento de la Cámara, presenta la siguiente **Proposición no de Ley para poner en marcha los controles al Sistema de Interceptación de las Comunicaciones (SITEL)**, utilizado por el Gobierno desde diciembre de 2004, para su debate en Pleno.

Madrid, 4 de Noviembre de 2009



Fdo.: Soraya SAENZ DE SANTAMARIA ANTON

Portavoz



Fdo.: Esteban GONZALEZ PONS

DIPUTADO

GRUPO PARLAMENTARIO POPULAR EN EL CONGRESO

Las comunicaciones electrónicas constituyen la infraestructura por la que se construye la sociedad del conocimiento, pero el crimen organizado se sirve también de ellas. En momentos en los que la sociedad está siendo castigada con frecuencia por determinados delitos que generan especial alarma social, se puede tener la tentación de establecer un sistema en el que el afán de control prime sobre la libertad en las comunicaciones, sacrificando los derechos civiles, y comprometiendo gravemente el ejercicio de las libertades individuales.

SITEL es un avanzado sistema informático gestionado por el Ministerio del Interior, que permite la interceptación de las comunicaciones y la recogida de un conjunto de datos conocidos como "*información asociada a la comunicación*". Estos datos incluyen los generados por la propia comunicación, los datos de identificación como el IMEI (identidad internacional de cada equipo móvil) o el IMSI (identidad internacional del abonado a un móvil), que hacen posible seguir interceptando una comunicación, aunque se cambie de teléfono o de tarjeta SIM, también la localización geográfica de los interlocutores o el tráfico de llamadas, los mensajes SMS, accesos a Internet e información generada por la navegación en Internet. Es decir, se aporta mucha más información sobre la persona a la que se investiga que la mera conversación a la que generalmente se refiere el juez cuando autoriza una interceptación telefónica. No sólo se puede vulnerar el derecho de las comunicaciones, sino también el derecho a la intimidad.

El Gobierno como consecuencia del desarrollo de las nuevas redes de comunicación electrónica y del auge de la telefonía móvil, se planteó en 2001 la necesidad de mejorar los sistemas de interceptación de las comunicaciones adaptándolas a las nuevas tecnologías. Eso supuso una doble actuación, por un lado tecnológica, para generar el software y por otra jurídica, para adecuarlo

GRUPO PARLAMENTARIO POPULAR EN EL CONGRESO

a nuestro Ordenamiento. Para hacerlo, pidió informes sobre la legalidad del mismo a los Ministerios de Justicia y Defensa además de al Consejo General del Poder Judicial. Dichos informes pusieron de manifiesto importantes deficiencias en la cobertura legal para ponerlo en funcionamiento, entre ellas, la necesidad de que se aprobase una Ley Orgánica para regular esta materia.

Esto supuso la paralización de su implantación, aunque el sistema comenzó a utilizarse en diciembre de 2004. Posteriormente para darle cobertura legal se dictó un Reglamento, el R.D. 424/2005, de 15 de abril, en desarrollo de la Ley General de Comunicaciones, Ley 33/2003, de 3 de noviembre, y más tarde una insuficiente Ley de carácter ordinario, la Ley 25/2007, de conservación de datos relativos a las comunicaciones que modifica, en su disposición final, el artículo 33 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Además de la falta de carácter orgánico, presenta rasgos de dudosa constitucionalidad. Así, en el apartado 8º) obliga a las operadoras de telefonía a facilitar datos personales de sus clientes a la policía con carácter previo a la orden de interceptación y en el 6º y 7º a facilitar información sensible aunque la orden de interceptación no lo solicite.

Por otra parte, hay que tener en cuenta que los soportes originales de las grabaciones que en este momento se están utilizando de SITEL y se aportan a los Tribunales, no están firmadas electrónicamente ni garantizadas por ninguna autoridad que garantice su autenticidad, incumpliendo por tanto los requisitos exigidos por la Ley 59/2003, de 19 de diciembre, de firma electrónica que exige la existencia de garantías sobre la autenticidad y la encriptación para evitar filtraciones indeseadas.

No discutimos que SITEL y la tecnología en general pueda ser un eficaz medio para combatir la criminalidad, pero el Estado de Derecho exige además de un fin loable, legalidad, proporcionalidad de los medios utilizados en la

GRUPO PARLAMENTARIO POPULAR EN EL CONGRESO

investigación y respeto a las garantías constitucionales. En este sentido, la extracción de información sobre las comunicaciones y la vida privada de los ciudadanos debe respetar escrupulosamente todas las exigencias de legalidad constitucional, pues en otro caso, la intromisión en la esfera de la privacidad de las personas quedaría invalidada como medio de prueba, cuestión ésta a la que no podemos ceder.

Por cuanto antecede, el Grupo Parlamentario Popular en el Congreso, formula la siguiente Proposición no de Ley:

- 1º. El Congreso de los Diputados insta al Gobierno a remitir a la Cámara, en el plazo de dos meses, un Proyecto de Ley Orgánica que regule la interceptación de las comunicaciones.

Dicha regulación deberá establecer, entre otras, las siguientes medidas:

- La exclusiva competencia de la autoridad judicial para la gestión de todos los sistemas y software de interceptación de las comunicaciones entre los ciudadanos.
- La designación de un funcionario responsable identificado de los centros de interceptación de las comunicaciones y de cada interceptación.

La utilización de estos sistemas y software para interceptar y grabar las comunicaciones requerirá:

- Que el juez especifique en la Resolución qué sistema de interceptación se debe utilizar.

GRUPO PARLAMENTARIO POPULAR EN EL CONGRESO

- Que el juez especifique y motive individualizadamente qué datos además del contenido de la comunicación deben ser interceptados.
- En el supuesto que por cuestiones técnicas se acceda a datos no autorizados, éstos deberán destruirse de forma inmediata.
- La destrucción obligatoria de forma fehaciente de cualquier soporte informático en el que pudieran haber quedado registradas las grabaciones que no se incorporen al procedimiento.
- Los soportes digitales en los que se realice la grabación de datos deberán estar firmados por una autoridad certificadora de autenticidad para evitar la manipulación de los datos grabados. Al mismo tiempo, la entrega de los ficheros digitales a la autoridad judicial también deberá estar firmada electrónicamente para evitar su manipulación y encriptada para evitar filtraciones, de forma que esos discos se constituyan en originales "evidencia legal", tal y como exige el Tribunal Europeo de Derechos Humanos. Una vez aportados al proceso, deberán destruirse todas las copias existentes, incluido los datos obrantes en los servidores de SITEL.

GRUPO PARLAMENTARIO POPULAR EN EL CONGRESO

- Limitar la autorización de la interceptación a un mes con prórrogas de quince días hasta un período máximo de un año. Tanto la autorización como las prórrogas sucesivas deberán revestir la forma de auto y estar suficientemente motivadas.
- Regular con carácter específico las investigaciones referentes a los delitos de terrorismo, crimen organizado, narcotráfico, pederastia y pornografía infantil que, dentro del respeto a la Ley, garantice la mayor eficiencia en la lucha contra estas graves formas de delincuencia.
- La Comisión de Control de los Créditos Destinados a Gastos Reservados del Congreso de los Diputados conocerá, con carácter anual, un informe sobre la utilización del Sistema de Interceptación de las Comunicaciones, SITEL, y otros software similares que le puedan sustituir, sin perjuicio de las facultades que corresponden a las autoridades judiciales.

2º La Comisión de Justicia del Congreso de los Diputados antes de un año elaborará un informe sobre el impacto de las innovaciones tecnológicas en los derechos civiles al ser utilizadas por la Administración Pública.