

Asociación de Internautas



Quando la democracia empieza a perder su alma



Por su notable interés reproducimos íntegramente la ponencia que sobre el sistema de interceptación de las comunicaciones, Sitel, presentó Pedro Martínez, Fiscal del Tribunal Superior de Madrid, ante la Conferencia Mundial sobre Privacidad, celebrada en Madrid.

Buenas tardes

En primer lugar quiero agradecer a los organizadores la invitación para participar en esta [Conferencia Mundial sobre Privacidad](#).

Nos encontramos en unos momentos difíciles y no sólo por la crisis financiera y económica que estamos atravesando. También, y sin darnos cuenta hemos caído en una crisis moral provocada por un afán de bienestar, y, un consumo desmesurado que ha terminado por incorporar la seguridad a la bolsa de la compra. Sin embargo todo esto nos está haciendo perder valores esenciales que hacen peligrar la sociedad de las libertades transformándola en una sociedad cada vez más vigilada.

Lo más grave es que este fenómeno se produce de forma global. En los aeropuertos de todo el mundo se nos somete a torturas de seguridad, para darnos confianza y se transmiten datos de unos Estados a otros, referentes a los registros de pasajeros (PNR). Datos que el viajero, no siempre conoce ni consiente.

Pero también los Gobiernos para mejorar la seguridad se ceden e intercambian información, mediante convenios gubernamentales de cesión e intercambio de información que no son controlados por los Parlamentos Nacionales respectivos. También se crean espacios comunes de vigilancia y de interceptación de comunicaciones electrónicas, de forma que se intercepta en un Estado una comunicación por encargo de otro Estado parte en el convenio.

En Europa, todo comienza con la Resolución sobre Interceptación Legal de las Comunicaciones de la Unión Europea, (1995) y termina

Quando la democracia empieza a perder su alma

esta primera etapa aproximadamente con la aprobación de su sucesora (19 Mayo 1999), que fue la que dio a conocer la palabra Enfopol al mundo.

1ª Etapa: Concretamente el 7 de Mayo de 1999, el Parlamento Europeo aprobó la Resolución del Consejo sobre interceptación legal de las comunicaciones relativo a las nuevas tecnologías. Más conocido como Resolución Enfopol, y se abre el camino a un sistema de interceptación y vigilancia de las comunicaciones en todo el territorio de la Unión Europea.

La extensión de los poderes otorgados a las policías europeas mediante este plan, unido al secretismo que ha rodeado su gestación y desarrollo, lo convierten en una grave amenaza potencial para la intimidad en la Europa del nuevo milenio.

Periodo intermedio: 1999-2000, en este periodo la redacción de documentos Enfopol y Resoluciones sobre interceptación legal se reduce fuertemente como consecuencia de la mala publicidad generada y la falta de apoyo político público. Mientras tanto, se debate y aprueba el Convenio sobre Asistencia Mutua en Materia Penal entre los Estados Miembros de la Unión Europea, de 29 de mayo del 2000, que dedica el Título III a la Intervención de las telecomunicaciones, y autoriza las interceptaciones electrónicas a nivel europeo.

La web oficial de la Unión Europea sintetiza la cuestión referente a la Interceptación de telecomunicaciones así:

La interceptación de una comunicación podrá ser efectuada, a petición de la autoridad competente de otro Estado miembro, por una autoridad judicial o administrativa designada por el Estado miembro en cuestión. La telecomunicación podrá interceptarse y transmitirse directamente al Estado miembro demandante, o ser registrada y transmitida con posterioridad.

Es decir admite la posibilidad de que puedan ordenarse o realizarse interceptaciones por orden gubernativa sin autorización judicial. Esto es un retroceso importante en el Estado de Derecho.

Aunque los Requisitos Enfopol no son mencionados explícitamente, en el Convenio se supone que serán empleados para fijar el tipo y extensión de las intervenciones policiales.

2ª Etapa: Tiene por objetivo consolidar el referido Convenio sobre Asistencia Mutua en Materia Penal. Su principal aportación es la Directiva 2006/24/CE, de 15 de Marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por la que se modifica la Directiva 2002/58/CE.

Quando la democracia empieza a perder su alma

Esta norma establece la obligación para las compañías de telecomunicaciones de retener por un periodo de entre 6 y 24 meses numerosos datos de comunicaciones telefónicas, tanto fija como móvil, de telefonía por Internet y de Internet de todos los ciudadanos.

La Directiva nos convierte a todos los ciudadanos en sospechosos, no diferencia entre el ciudadano honesto y responsable y el delincuente, por consiguiente su objetivo no es controlar al delincuente sino al ciudadano, es pues una norma de control social como han denunciado numerosas asociaciones de derechos civiles de toda Europa y nosotros aprovechamos la ocasión para reiterarlo.

En España es a partir los atentados del 11 de septiembre de 2001 cuando el Gobierno, (entonces de la derecha) se implicó decididamente en este proyecto sobre interceptación legal de las comunicaciones.

De tal forma que adquirió, desarrollo e implanto el software de interceptación de las comunicaciones electrónicas conocido como SITEL, (versión española de ENFOPOL), aunque no llegó a activarlo por existir informes que exigían una tramitación Parlamentaria del proyecto en forma de Ley Orgánica.

Tras los atentados de Madrid del 11 de Marzo de 2004, la izquierda gana las elecciones y con todo un discurso sobre el buen gobierno, la ética, la transparencia, la nueva forma de hacer política, activo el sistema, y lo generalizo, sin debate público alguno, sirviéndose de engaños para ocultar o al menos disimular su existencia.

En una primera fase se utilizó con carácter general sin norma jurídica alguna que le diera cobertura y después se incluyó en un reglamento sobre cuestiones operativas referentes a las telecomunicaciones, y por último debido a la presión judicial lo incluyó en una norma de insuficiente jerarquía y dudosa constitucionalidad.

El sistema de interceptación de las comunicaciones, (Sitel) no cumple los requisitos de una sociedad democrática para poder actuar. No ha existido nunca debate parlamentario sobre su implantación y sus límites, ni tampoco debate social, ya que se introdujo en secreto mediante disposiciones de ínfimo rango normativo que fueron aprobadas directamente por el Gobierno evitando todo trámite de información pública.

Por otra parte aunque en España son los jueces los que deben autorizar las interceptaciones, no existe un control judicial efectivo como exige el Tribunal Europeo de Derechos Humanos. Por lo siguiente:

1º Los jueces no han recibido información y formación en esta

Quando la democracia empieza a perder su alma

tecnología.

2° Las operadoras de telefonía deben facilitar con carácter previo a la orden de interceptación determinados datos personales de sus clientes.

3° Las operadoras de telefonía deben facilitar determinados datos personales de sus clientes incluida la localización de los interlocutores aunque los jueces no la ordenen expresamente.

4° No existe garantía alguna de la autenticidad de la información que se aporta a la los Juzgados, ya que se entrega en discos sin firma electrónica y sin encriptar.

5° Toda la información que interceptan queda almacenada en unos servidores que se encuentran en los llamados Centros de Interceptación de las Comunicaciones disposición del poder ejecutivo.

La aplicación de la Directiva en Europa sobre conservación y cesión de datos de las comunicaciones electrónicas es irregular.

Existen Países que no la han acogido en sus Ordenamientos Jurídicos, y los que lo han hecho ha sido de forma desigual. España ha sido pionera y rigurosa en su incorporación, admite el plazo máximo de un año para conservar los datos y no regula un sistema de control judicial efectivo, permitiendo que los datos puedan ser cedidos por razones de seguridad al Centro Nacional de Inteligencia, y una vez en su poder nada impide que puedan ser transmitidos a terceros Estados, ya que la Ley no prohíbe esta cesión, ni requiere la necesidad de autorización judicial para efectuarla. De hecho existen convenios con terceros Países que amparan la cesión de esos datos.

La sociedad de la vigilancia ha llegado sin que casi nos hayamos dado cuenta. En parte, resulta esencial para facilitar los servicios que necesitamos. En parte, resulta cuestionable y, puede resultar injustificable, intrusiva y opresiva. Pero lo más alarmante es la forma como se ha introducido, sutil e imperceptiblemente. De hecho la mayoría de la gente no sabe nada, o muy poco sobre la sociedad de la vigilancia: se percibe como historias de ciencia ficción, no de la vida cotidiana. Y, en consecuencia, se ha generado muy poco debate público sobre la misma. Los medios apuestan por el entretenimiento y apenas hacen preguntas, no saben o no entienden lo que esta pasando y siguen enfocando su luz sobre otros asuntos, y eso los conduce a la parcialidad moral. Mientras tanto la sociedad de las libertades se deteriora cada día más.

Pocos van a discutir que el Estado no utilice la tecnología para la lucha contra la delincuencia. Pero el Estado de Derecho, no puede usar armas que no sean legítimas a menos que la sociedad empiece a

Quando la democracia empieza a perder su alma

perder su alma democrática. Al contrario, es imprescindible la transparencia, por eso las medidas a utilizar, además de respetuosas con el régimen de garantías, deben ser públicas y conocidas, pues es la única forma que tiene el ciudadano para exigir el cumplimiento de la ley y el respeto de sus derechos.

En este panorama sombrío alguna luz se vislumbra. Me refiero a la nueva ruta emprendida por el presidente de EE. UU, Barack Obama que en consonancia con lo prometido en su campaña, el día uno de su mandato firmó una orden ejecutiva y dos memorandos presidenciales anunciando lo que él calificó como una nueva era de apertura . La orden ejecutiva revocaba los cambios hechos por el Presidente W Bush en la Ley de Documentos Presidenciales, y los dos memorandos propugnan la apertura de la administración y la libertad de información. En una palabra, el fin del secretismo sobre los actos de Gobierno y Administración.

Esperemos que esta nueva era de apertura no sólo se consolide en EE. UU sino que también se extienda al resto del mundo y que la sociedad recupere su alma democrática.

MUCHAS GRACIAS POR SU ATENCIÓN

Ampliar información sobre la interceptación de las telecomunicaciones

[Saber más sobre la Interceptación de las Comunicaciones en España](#)

2019 ©Asociación de Internautas