I. SITEL : Sentencia del Tribunal Supremo (Sala de lo Penal) nº 1.078/2009 de 5-11-2009 (Recurso de casación nº 419/2009)

Fundamentos de Derecho :

OCTAVO.-Afirma el recurrente que dicho sistema (SITEL) es inconstitucional y se queja de la deficiencia en el rango normativo regulador de las intervenciones telefónicas en nuestro ordenamiento.

Más directamente la aceptabilidad del sistema ha sido objeto de examen en nuestra Sentencia 23 de marzo de 2009 en el recurso 1732/2008 en la que dijimos: Lo que interesa para este proceso penal ....a los efectos del derecho a un proceso con todas las garantías del art. 24.2 CE , es si estas garantías se respetaron en el momento de su obtención y en el de su incorporación a las actuaciones, lo que ciertamente así ocurrió como nos explica la sentencia recurrida en sus páginas 24 y 25.

Y se añade: La cuestión planteada en este motivo 7º es un tema que interesa a la Administración y al Poder Legislativo, a los efectos de determinar el sistema a seguir para conservar (o no conservar) y controlar las conversaciones telefónicas legalmente intervenidas y grabadas, que ahora quedan integradas en un solo archivo mediante el referido sistema SITEL, que ha venido a sustituir a las anteriores audiciones personales e individualizadas que realizaban los correspondientes agentes policiales.

Por eso fue la Sala de lo Contencioso-Administrativo de este Tribunal Supremo la que tuvo que pronunciarse sobre este problema en su sentencia de 5 de febrero de 2008 en respuesta a una demanda planteada por la Asociación de Internautas, citada en el propio escrito de recurso.

Ratifica esta Sentencia el criterio ya expuesto en la Sentencia de 13 de marzo de 2009 en el recurso 10624/2008 en la que se expuso: El programa SITEL es una implementación cuya titularidad ostenta el Ministerio del Interior. Su desarrollo responde a la necesidad de articular un mecanismo moderno, automatizado, simplificador y garantista para la figura o concepto jurídico de la intervención de las comunicaciones.

El sistema se articula en tres principios de actuación:

1. Centralización: El servidor y administrador del sistema se encuentra en la sede central de la Dirección General de la Guardia Civil, distribuyendo la información aportada por las operadoras de comunicaciones a los distintos usuarios implicados.
2. Seguridad: El sistema establece numerosos filtros de seguridad y responsabilidad, apoyados en el principio anterior. Existen 2 ámbitos de seguridad:

*Nivel central: Existe un ordenador central del sistema para cada sede reseñada, dotado del máximo nivel de seguridad, con unos operarios de mantenimiento específicos, donde se dirige la información a los puntos de acceso periféricos de forma estanca. La misión de este ámbito central es almacenar la información y distribuir la información.

*Nivel periférico: El sistema cuenta con ordenadores únicos para este empleo en los grupos periféricos de enlace en las Unidades encargadas de la

investigación y responsables de la intervención de la comunicación, dotados de sistema de conexión con sede central propio y seguro. Se establece codificación de acceso por usuario autorizado y clave personal, garantizando la conexión al contenido de información autorizado para ese usuario, siendo necesario que sea componente de la Unidad de investigación encargada y responsable de la intervención.

3. Automatización: El sistema responde a la necesidad de modernizar el funcionamiento de las intervenciones de las comunicaciones, dotándole de mayor nivel de garantía y seguridad, reduciendo costes y espacio de almacenamiento, así como adaptarse al uso de nuevos dispositivos de almacenamiento.

c) Información aportada por el sistema.

El sistema, en la actualidad, aporta la siguiente información relativa a la intervención telefónica:

1. Fecha, hora y duración de las llamadas.
2. identificador de IMEI y nº de móvil afectado por la intervención.
3. Distribución de llamadas por día.
4. Tipo de información contenida (SMS, carpeta audio, etc.)

En referencia al contenido de la intervención de la comunicación, y ámbito de información aportada por el sistema, se verifica los siguientes puntos:

1. Repetidor activado y mapa de situación del mismo.
2. Número de teléfono que efectúa y emite la llamada o contenido de la información.
3. Contenido de las carpetas de audio (llamadas) y de los mensajes de texto (SMS).

d) Sistema de trabajo.

Solicitada la intervención de la comunicación y autorizada esta por la Autoridad Judicial el empleo del Programa SITEL, la operadora afectada inicia el envío de información al Servidor Central donde se almacena a disposición de la Unidad encargada y solicitante de la investigación de los hechos, responsable de la intervención de la comunicación.

El acceso por parte del personal de esta Unidad se realiza mediante código identificador de usuario y clave personal. Realizada la supervisión del contenido, se actúa igual que en el modo tradicional, confeccionando las diligencias de informe correspondientes para la Autoridad Judicial. La EVIDENCIA LEGAL del contenido de la intervención es aportada por el Servidor Central, responsable del volcado de todos los datos a formato DVD para entrega a la Autoridad Judicial pertinente, constituyéndose como la única versión original.

De este modo el espacio de almacenamiento se reduce considerablemente, facilitando su entrega por la Unidad de investigación a la Autoridad Judicial competente, verificándose que en sede central no queda vestigio de la información.

2. Comentario-análisis de esta sentencia

De los poquísimos datos conocidos sobre Sitel- materia secreta donde las haya, como es lógico- , de esta Sentencia parece decirse que el procedimiento de trabajo de Sitel sería éste :

1º.- Se solicita y obtiene autorización judicial para que se active Sitel, respecto a una concreta(s) persona(s). La autorización judicial llega al Ministerio del Interior, presumiblemente en papel y/o mediante Fax ,correo electrónico . A estos efectos da igual, pues se verá que cualquiera de estas vías tradicionales de comunicación, no son suficientes para garantizar la finalidad u objetivo de la previa autorización judicial.

Esa finalidad consiste en que el Sistema Sitel NO PUEDA iniciar sus transacciones para interceptar las comunicaciones de una persona concreta, SIN QUE el Sistema Sitel se cerciore de que la autorización viene del Juez X, y sin que esa autorización quede registrada dentro de Sitel. Es decir, Sitel no podrá empezar a interceptar comunicaciones de la persona Z, SI PREVIAMENTE no se ha cargado en Sitel la autorización judicial .

2º.- Un usuario del Ministerio del Interior recibe la autorización judicial – en papel, fax, correo electrónico - , y la introduce él personalmente (NO el Juez) en el Sistema . Aquí hay un primer riesgo evidente : que por "error voluntario o involuntario, se grabe en Sitel una autorización judicial inexistente . Para evitar estas posibles suplantaciones de personalidad, hace mucho que se ha inventado la solución :

Que es muy sencilla : lo primero es diseñar el Sistema informático con dos controles o filtros de acceso . Uno primero – es previo y primero en el tiempo, pues sin él no se "entra" materialmente en el Sistema informático – es el control del acceso físico . Se trata de asegurarse de que quien entra en el Sistema, es realmente él, y no otra persona . Ese acceso físico suele constar de dos claves : una, la clave de usuario autorizado ; y otra, la clave personal , contraseña o password. Con el DNI electrónico o digital, por ejemplo, puede autenticarse la identidad personal de quien accede al Sistema .

Pasado este primer pórtico, el usuario sí ha entrado en el Sistema, pero sólo para ver en pantalla el menú de las transacciones de éste. Todavía no podrá iniciar ninguna de éstas transacciones , si antes no se activa el segundo control de accesos, que es el control lógico . Este segundo filtro, que es el decisivo, nos indica a qué aplicaciones o transacciones concretas puede acceder el usuario X, que previamente identificado como tal, ha entrado al Sistema.

3º.- En Sitel parece que la operatoria es la siguiente : una vez grabada en Sitel la autorización judicial – grabación realizada por persona del Ministerio del Interior - , ya se empezaría a interceptar las comunicaciones de la persona Z.

Aparentemente esto sería correcto, y legal. Así se lo ha parecido al Tribunal Supremo. Pero es sólo apariencia, porque cualquier persona medianamente enterada de cómo funcionan los Sistemas de Información, detecta enseguida los siguientes fallos o riesgos de seguridad de un Sistema Sitel así operante :

A.- El fallo más inmediato y visible es que la autorización judicial no se introduce en Sitel directamente por el Juez , sino por otra persona dependiente del Mº del Interior. Esa persona , lógicamente, tendrá acceso propio a Sitel : entrará con su propia identidad , y lo más probable es que en pantalla le aparezca una opción titulada " Autorización judicial " , donde aparecerán varios campos vacíos , referidos a los datos identificativos de dicha autorización : Nombre y apellidos del Juez, fecha y número de

la autorización, etc...Esa persona de Interior introducirá allí los datos de la autorización judicial recibida.

Pero aquí está la trampa : en esa introducción "manual" de datos puede haber "fallos " : el más grave podría ser que se introdujeran datos de una autorización inexistente. Si el Sistema está programado para pasar a la fase siguiente, bastando para ello rellenar esos datos, pues la posibilidad de trampa está servida. El Sitel debería estar diseñado de forma que la autorización judicial sólo pudiera "entrar " en Sitel directamente desde el Sistema informático judicial , de forma que fuera el Juez autorizante quien, personalmente, y con su DNI electrónico o mecanismo seguro equivalente (certificado digital de FNMT, etc...) , procediera a introducir su autorización en Sitel por vía telemática.

B.- Pero más grave aún que eso, es el siguiente "agujero" : El Poder Judicial debe tener la seguridad de que Sitel está diseñado de la siguiente forma :

El sistema Sitel NO puede técnicamente empezar a funcionar, es decir, no puede empezar a interceptar comunicaciones, si previamente no se ha grabado en Sitel la autorización judicial preceptiva, en la forma recién señala. Esa instrucción debe estar grabada dentro del sistema operativo y dentro del programa de Sitel. Ahora mismo no sabemos si Sitel está diseñado así. Porque puede ocurrir que Sitel no esté programado con ese mecanismo de seguridad.

Puede ocurrir que Sitel , técnicamente, pueda realizar interceptaciones, sin que ANTES se haya introducido en Sitel la preceptiva autorización judicial. Los Jueces tienen que controlar , no sólo los accesos individualizados, sino el programa informático que posibilita esos accesos de Sitel en la práctica . Porque es de niños, es ilusorio pensar que basta con autorizar individualmente cada caso . Porque TODOS los casos pasan , todos ellos, por el mismo filtro, que es el programa informático de Sitel. Y éste es el que tienen que controlar los Jueces.

Ese control judicial del programa informático de Sitel debe estar establecido por la correspondiente Ley , orgánica si es preciso. Porque si no se da ese control , el riesgo es inmenso . Se puede dar lo siguiente : que el Poder judicial haya dado su conformidad o visto bueno al programa informático de funcionamiento de Sitel , y, a pesar de ello, el Ministerio del Interior decida cambiar ese programa al día siguiente, sin contar con dicho Poder judicial, en el sentido de posibilitar que Sitel actúe sin necesidad de que previamente se haya grabado en Sitel la autorización judicial individualizada correspondiente, autenticada y con todas sus garantías.

Por eso el control judicial del programa informático , de la aplicación Sitel , debe ser completo, permanente y continuo . Blog

1. Antes de ponerse en marcha por primera vez , Sitel debería haber sido auditado informáticamente en este aspecto por el Poder judicial. No se ha hecho, pero eso no quiere decirse que no deba hacerse ya, con carácter de urgencia.
2. Cualquier modificación posterior de dicho programa, requerirá la previa conformidad del Poder judicial, que éste realizará , en su caso, tras haber analizado y auditado dicha modificación del programa.
3. El Poder judicial deberá tener acceso directo e inmediato a Sitel, a los solos efectos de poder comprobar si su programa se ha cambiado o no. Esa auditoría o control informático permanente, realmente es la única garantía de que las autorizaciones judiciales individuales no se conviertan en papel mojado.

CONCLUSION:

Hace falta airear las reformas que se necesitan : aparte de las reformas constitucional y de nuestro Poder judicial, la de dictar una ley, orgánica, que establezca la necesidad de un control judicial riguroso sobre Sitel y sistemas similares, simplemente sobre la base realista de lo que cualquier persona medianamente enterada en Informática ya conoce. Nuestras leyes deben estar enraizadas en nuestra realidad social – ésta se configura hoy en base a la Informática- , y no como ahora lo están ,ancladas en la era del papel. Porque nos jugamos nuestras libertades fundamentales.