# DOS INTERVENCIONES SOBRE INVESTIGACIÓN PENAL Y DATOS PERSONALES

Este artículo recoge de manera conjunta las intervenciones de la directora del Centro de Estudios Jurídicos y Formación Especializada y de la directora de la Agencia Catalana de Protección de Datos realizadas en las Jornadas sobre Jueces, Fiscales y Policías, vértice de este número de la Revista.

Si bien, por un lado, la intervención de la primera trata los puntos fuertes y débiles del Sistema Integrado de Interceptación de las Telecomunicaciones (SITEL) en cuanto a la validez y eficacia de las pruebas obtenidas mediante este sistema en el proceso penal, la segunda aborda la protección y el tratamiento de los datos obtenidos durante la investigación penal por parte de las fuerzas y cuerpos de seguridad.

Aunque el sistema SITEL permite recoger una gran cantidad de información mediante la intervención de las comunicaciones en tiempo real, plantea una serie de incertidumbres respecto al tratamiento posterior de los datos obtenidos. Este tratamiento, al menos, debería respetar siempre los límites impuestos por la Ley 15/1999, de 13 de diciembre, de protección de datos personales y la regulación específica aplicable al tratamiento de datos por parte de las fuerzas de seguridad.

*This article brings together the presentation made by the Director of the* Centre d'Estudis Jurídics i Formació Especialitzada *(Centre for Legal Studies and Specialist Training) and the Director of the* Agència Catalana de Protecció de Dades *(Catalan Data Protection Agency) at the conferences on Judges, Prosecutors and the Police, the theme of this edition of the Journal.*

*While, on the one hand, the paper given by the former Director deals with the strong points and weaknesses of the* Sistema Integrat d'Intercepció de les Telecomunicacions *(The Integrated System of Interception of Telecommunications, or SITEL) in terms of the validity and effectiveness of evidence obtained through SITEL system, in legal proceedings, the latter Director looks at the protection and processing of data obtained, in criminal investigations, by the police and other security forces.*

*Although the SITEL system does allow one to gather a large amount of information through intervention of communications in real time, it generates a number of questions about how this information might then be used. The way the information is processed must respect, at the very least, the limits set by Law 15/1999, of 13 December, on the Protection of Personal Data and also by specific regulations applicable to the use of information by the security forces.*







## EL SISTEMA INTEGRADO DE INTERCEPTACIÓN LEGAL DE LAS TELECOMUNICACIONES (SITEL)

ROSER BACH I FABREGÓ

Directora del Centro de Estudios Jurídicos y Formación Especializada. Generalitat de Cataluña

### 1. INTRODUCCIÓN

En primer lugar me referiré al Sistema Integrado de Interceptación de las Telecomunicaciones (SITEL), fijándome especialmente en la recepción efectuada

en la jurisprudencia de la Sala Segunda del Tribunal Supremo, porque en definitiva nos dará las claves de cuáles son los problemas más importantes que se plantean en el proceso penal, en concreto sobre la validez y la eficacia probatoria de las evidencias obtenidas a través de este sistema de interceptación de las comunicaciones y de las soluciones que se proponen, y también de los problemas que no se han planteado y que a buen seguro aparecerán.

Fue alrededor del año 2000, cuando ya existía un auge extraordinario en la utilización de la telefonía móvil y, consecuentemente, de su uso por parte de la delincuencia organizada, cuando se puso de manifiesto la falta de operatividad y las dificultades prácticas para llevar a cabo las intervenciones telefónicas con los sistemas de interceptación tradicionales.

A este respecto, el Gobierno del Estado encargó a una empresa especializada la creación de un sistema que pudiera resolver los problemas de efectividad en las interceptaciones de las comunicaciones.

Este nuevo sistema debía permitir el cambio de un sistema manual a un sistema digital, la interceptación y la escucha de las comunicaciones en tiempo real, la capacidad de almacenar todas las conversaciones efectuadas a través de los números intervenidos y, al mismo tiempo, proporcionar una gran cantidad de información complementaria, como por ejemplo la identidad y la localización física de las personas interlocutoras, el IMEI[1] de los terminales, los mensajes SMS, etc.

Después de diversos intentos para ponerlo en marcha, con una propuesta de Reglamento, y con la aparición de dos informes contrarios al nuevo sistema (de la Agencia Española de Protección de Datos y del Consejo General del Poder Judicial), finalmente se puso en marcha en el año 2004.

Mediante el Real decreto 424/2005, de 15 de abril, se aprobó el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.

Como ya he adelantado antes, la recepción en la jurisprudencia de la Sala Segunda del Tribunal Supremo puede darnos una idea de los problemas que se plantean y que se plantearán en un futuro en relación con este sofisticado sistema de interceptación de las comunicaciones, y más si tenemos en cuenta que finalmente habrá que analizar la valoración de los datos obtenidos con la utilización del SITEL como pruebas, y también teniendo en cuenta que, a mi parecer, hay un gran desconocimiento en los juzgados y en los tribunales del funcionamiento real de este nuevo sistema, a pesar del tiempo que hace que ya está implantado.

Los aspectos esenciales que se tratan en las resoluciones dictadas hasta el momento son los que expongo en los siguientes apartados.

1. El IMEI es el identificador único a escala mundial que se da a cada terminal de un sistema de comunicación móvil. Las siglas corresponden a la denominación inglesa *international mobile equipment identity* (identificador internacional de equipamiento móvil) [n. de la ed.].

## 2. FUNCIONAMIENTO OPERATIVO DEL SISTEMA SITEL

En la Sentencia del Tribunal Supremo (STS) de 13 de marzo de 2009 se hace una extensa explicación del funcionamiento del sistema SITEL.

El SITEL es una implementación sobre la que ejerce la titularidad el Ministerio del Interior. Su desarrollo responde a la necesidad de articular un mecanismo moderno, automatizado, simplificador y garante de la figura o el concepto de la intervención de las comunicaciones.

El sistema se articula en tres principios de actuación:

*a) Centralización*

El servidor y administrador del sistema se encuentra en la sede central de la Dirección General de la Policía y la Guardia Civil, que distribuye la información aportada por las operadoras de comunicaciones a los diversos usuarios implicados.

*b) Seguridad*

El sistema establece numerosos filtros de seguridad y responsabilidad basados en el principio anterior. Hay dos niveles de seguridad:

— *Nivel central*

Dispone de un ordenador central del sistema para la sede reseñada, dotado del máximo nivel de seguridad, con unos operarios específicos de mantenimiento, desde donde se dirige la información a los puntos de acceso periféricos de forma estanca. La misión de este nivel central es almacenar la información y distribuirla.

— *Nivel periférico*

El sistema cuenta con ordenadores únicos para este uso en los grupos periféricos de enlace en las unidades encargadas de la investigación y responsables de la intervención de la comunicación, dotados de un sistema de conexión con la sede central propia y segura. Se establece una codificación de acceso para el usuario autorizado y una clave personal, que garantiza la conexión al contenido autorizado de información para este usuario, que tiene que ser forzosamente componente de la unidad de investigación encargada y responsable de la intervención.

*c) Automatización*

El sistema responde a la necesidad de modernizar el funcionamiento de las intervenciones de las comunicaciones, para dotarlo de un nivel mayor de garantía y seguridad, reducir costes y espacio de almacenamiento, así como para adaptarse al uso de nuevos dispositivos de almacenamiento.

La información relativa a datos telefónicos que en la actualidad aporta el sistema es la siguiente:

— fecha, hora y duración de las llamadas
— identificador de IMEI y número de móvil afectado por la intervención

— distribución de las llamadas por día
— tipo de información contenida (SMS, carpeta de audio, etc.)

Por lo que se refiere al contenido de la intervención de la comunicación y al tipo de información aportada por el sistema, se verifican los siguientes puntos:

— repetidor activado y mapa de su situación
— número de teléfono que efectúa la llamada o contenido de la información
— contenido de las carpetas de audio (llamadas) y de los mensajes de texto (SMS)

En cuanto al sistema de trabajo, una vez se ha solicitado la intervención de la comunicación y la autoridad judicial ha autorizado el uso del programa SITEL, la operadora afectada inicia el envío de la 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 personal de esta unidad accede, como se ha dicho antes, mediante el código identificador de usuario y la clave personal. Después de supervisar el contenido se actúa igual que con el sistema tradicional, es decir, se elaboran las diligencias de informe correspondientes para la autoridad judicial. La evidencia legal del contenido de la intervención es aportada por el servidor central, desde el que se vierten y graban todos los datos en formato DVD, que se constituye como única versión original. De esta manera el espacio de almacenamiento se reduce considerablemente, cosa que facilita la entrega por parte de la unidad de investigación a la autoridad judicial competente, y también se verifica que en la sede central no queda vestigio de la información.

## 3. LA NECESIDAD DE PETICIÓN EXPRESA DE LAS INTERVENCIONES MEDIANTE EL SISTEMA SITEL A LA AUTORIDAD JUDICIAL

El SITEL permite un nivel de intervención muy superior a los sistemas tradicionales, especialmente en relación al grado de información que puede proporcionar. Como hemos visto antes, incluso es posible la localización física de la persona que efectúa la comunicación telefónica.

Esta potencialidad informativa determina que para la autorización de la intervención a los agentes policiales encargados de la investigación sea necesaria una petición especialmente detallada en dos sentidos.

De hecho, la STS de 17 de noviembre de 2009 afirma que el SITEL es un método avanzado y extremadamente invasivo de la intimidad, de manera que la petición policial ha de explicar, aunque sea sumariamente, cuáles son los objetivos que se pretenden alcanzar y las consecuencias del funcionamiento del sistema.

Así pues, en primer lugar, además de los requerimientos de determinación objetiva y subjetiva que ha establecido reiteradamente el Tribunal Constitucional, es preciso que en la solicitud policial, en el caso de que la intervención se pre-

tenda llevar a cabo con el sistema SITEL, se señale de forma expresa que la intervención se hará con este sistema —por otro lado, hecho habitual en la práctica— y, en segundo lugar, dentro de las amplias posibilidades que ofrece el sistema en cuanto a datos que pueden obtenerse, cuál será en este sentido el alcance de la intervención.

## 4. LA APORTACIÓN AL JUZGADO DE INSTRUCCIÓN DE LAS GRABACIONES EN FORMATO DVD

Con los sistemas tradicionales de intervención de las comunicaciones, una vez finalizada la intervención, las cintas o los soportes que contenían las grabaciones originales eran aportadas al juzgado de instrucción que había autorizado la medida.

En efecto, la jurisprudencia tanto del Tribunal Constitucional como del Tribunal Supremo exigía que la aportación de las cintas de las grabaciones fuera íntegra y original, de manera que —sin perjuicio de la selección que pueda realizar el juez instructor o los mismos policías encargados de la investigación— lo que sería determinante a efectos de dotar de valor probatorio las conversaciones es que las cintas originales fueran entregadas al juzgado de instrucción y estuvieran a disposición de las partes.

Se trataba de un requisito de carácter procesal que no afectaba a la regularidad de la injerencia en el derecho al secreto de las comunicaciones, pero sí a la virtualidad probatoria de las intervenciones telefónicas.

Con esta perspectiva cambia substancialmente el funcionamiento del SITEL. En efecto, con el nuevo sistema, una vez acordada la interceptación de las comunicaciones, ésta se realiza de forma automatizada y se hace una grabación también automatizada en el servidor central; cuando finaliza la intervención, la grabación se pasa a soporte DVD, que es lo que se aporta al juzgado de instrucción.

Por tanto, ya no se puede hablar propiamente de grabaciones originales, excepto de las que constarán en el disco duro del servidor central, y lo que siempre hay que aportar al juzgado de instrucción es la copia de la información grabada en formato DVD.

La jurisprudencia de la Sala Segunda se ha referido a este aspecto en diversas resoluciones sobre recursos, en los que precisamente se impugnaba que los agentes policiales actuantes no habían aportado al procedimiento las grabaciones originales, haciendo referencia a la exigencia ya nombrada de aportarlas con la tecnología tradicional.

Por ejemplo, la STS de 17 de noviembre de 2009 indica en relación a esta exigencia de aportación del soporte original que, con el sistema tradicional, nunca se había exigido el traslado a la sede judicial del soporte que albergaba la bobina de las cintas, que sería el equivalente al disco duro centralizado con el nuevo sistema de interceptación. Sin embargo, creo que la comparación es poco oportuna ya que, sin perjuicio de lo que se considere que debe aportarse al juzgado de instrucción, no puede equipararse la grabación original que se pide al soporte físico donde está contenida.

Esta sentencia también añade, incidiendo en la autenticidad de las grabaciones, que la automatización del sistema SITEL no exige la presencia permanente de una persona escuchando en tiempo real las conversaciones intervenidas, ya que con la nueva tecnología se sustituye esta presencia personal por un sistema de grabación de alta seguridad y de difícil —por no decir imposible— manipulación, sin que la persona que eventualmente la hiciera no fuera detectada por su clave y personalmente identificada con más seguridad que con un sistema tradicional de cintas analógicas.

Otras sentencias de la Sala Segunda, como la de 12 de noviembre de 2009, argumentan que el disco con el archivo sonoro procedente del servidor central certificado digitalmente ha de considerarse archivo original, con independencia de que se conserve el archivo sonoro matriz en el disco duro del servidor central.

En el mismo sentido, la STS de 13 de marzo de 2009 afirma que el DVD que contiene la grabación de los datos se constituye como la única versión original.

En este punto hay que hacer referencia al voto particular a la STS de 1 de febrero de 2009. Independientemente de que se compartan o no las afirmaciones y, sobre todo, las objeciones que se hacen en la sentencia al sistema SITEL, su lectura es interesante porque también se refiere al valor probatorio de los DVD que se aportan al procedimiento.

En la sentencia mayoritaria se desestima la impugnación de los recurrentes en el sentido de cuestionar la autenticidad de los DVD puestos a disposición del juez de instrucción que contienen las conversaciones telefónicas de las personas imputadas.

Señalan los magistrados que subscriben el voto particular que cuando se cuestiona esta autenticidad la respuesta no puede consistir en un acto de fe inspirado en las excelencias del *software* que utilizan los agentes policiales, ni tampoco puede convertirse en un debate sobre la credibilidad de las fuerzas y cuerpos de seguridad del Estado, sino que afirman que se trata de un problema de carácter jurídico, específicamente procesal, sobre el valor atribuible a estos soportes que constituyen una prueba electrónica. Por tanto, se trata de una problemática ajena a la suficiencia técnica del SITEL y al funcionamiento del sistema respecto al ámbito de la protección de datos. Se trata, como se ha dicho, de un problema procesal, del valor probatorio atribuible a los DVD que se incorporan al proceso.

El voto particular, en primer término, repasa las deficiencias regulativas por lo que respecta al control de la autenticidad e integridad del documento digital y, en segundo término, expone cuáles deberían ser los requerimientos del documento para satisfacer estas exigencias.

El voto particular hace un repaso de los supuestos en los que la Administración ha implantado la utilización de documentos electrónicos y los requisitos que ha establecido en la normativa reguladora correspondiente, como por ejemplo en el ámbito del notariado, en el ámbito del acceso electrónico de la ciudadanía al servicio público en el intento de crear una auténtica administración electrónica, o la documentación electrónica del juicio oral; ámbitos en los cuales el legislador no ha sido ajeno a las exigencias de autenticidad y ha establecido rigurosos requisitos que hacen referencia esencialmente a la firma electrónica.

Pues bien, el voto particular señala que, a la vista de la normativa que regula el sistema SITEL, todas estas garantías que tienden a preservar la autenticidad y la integridad de los documentos digitales sólo se han establecido en la relación que se produce entre los agentes de policía facultados y las operadoras de telefonía. En efecto, se establecen requisitos exigentes y formalidades técnicas en el flujo de información entre los servidores de telefonía y los agentes facultados, pero todo este sistema de garantías desaparece cuando los agentes facultados graban en un DVD las conversaciones que estiman relevantes y las presentan en el juzgado.

El voto particular continúa indicando que la implantación de un sistema que ofrece tantas posibilidades como el SITEL no debería haber prescindido de una idea tan elemental como la existencia de tres sujetos funcionales diferentes:

*a)* las operadoras de telefonía (sujetos obligados),
*b)* los funcionarios de policía (agentes facultados),
*c)* los jueces de instrucción que autorizan la interceptación y se convierten en los destinatarios últimos del resultado de las escuchas.

Y afirma que de esta manera el SITEL convierte a los juzgados y tribunales en «un punto débil», en «una tierra de nadie» en la que las garantías de seguridad e integridad del documento electrónico se degradan de forma insalvable; igualmente, afirma el voto particular, los juzgados de instrucción se convierten en simples receptores de unos soportes electrónicos cuyo contenido no puede basarse en ninguna otra garantía que no sea la confianza acrítica en la profesionalidad de los agentes que lo proporcionan. Del mismo modo, el secretario judicial, en su condición de fedatario, se ve obligado a subscribir un acto de aseveración a ciegas, no puede dar fe de que el contenido de los DVD coincida con el original al que no tiene acceso, ya que la oficina judicial no puede hacer un seguimiento de las interceptaciones.

Una vez expuestas las deficiencias en la regulación del sistema, el voto particular detalla los requisitos que deberían cumplir los documentos digitales en los que se incorporan las grabaciones que, evidentemente —indican—, constituyen la prueba electrónica.

Por lo que respecta al análisis de la autenticidad, los magistrados señalan que es necesario exigir dos niveles de autenticidad. En primer lugar el que garantice que, una vez grabada la conversación en el terminal custodiado por los agentes de policía, el fichero generado no ha sido abierto con posterioridad y por tanto no ha sido expuesto a ningún tipo de modificación. El segundo nivel deriva del hecho de que la prueba que se ofrece al tribunal está integrada no por los ordenadores centrales sino por copias incorporadas a uno o más DVD, de manera que un segundo nivel de seguridad consiste en el hecho de que, inmediatamente después de finalizado el proceso de grabación, se active una certificación que garantice que:

*a)* desde el momento en que se termina el proceso de grabación hasta que lo recibe el juzgado el DVD no ha sido abierto;

*b)* en consecuencia no ha existido riesgo de manipulación, y
*c)* quien garantiza la integridad del documento es el funcionario responsable del tratamiento y, por tanto, el único con capacidad de autentificación.

No obstante, los magistrados discrepantes reiteran que estas medidas de seguridad no se han previsto, de manera que el cumplimiento de estas exigencias es realmente complicado.

En este punto, pienso que puede concluirse que en el diseño del sistema debería haberse previsto la posibilidad —que técnicamente seguro que es factible— de que el órgano judicial pudiera tener acceso al servidor central, que es donde efectivamente se aloja la grabación original, o, si fuera necesario, a una certificación digital de integridad y autenticidad; de tal manera que el secretario judicial estuviera en condiciones de certificar la correlación del DVD entregado al juzgado de instrucción con la versión original, como se hacía tradicionalmente con el sistema ordinario de intervención.

## 5. LA CONSERVACIÓN DE LAS INTERVENCIONES Y LOS DATOS OBTENIDOS

Una de las cuestiones que adquiere una importancia significativa en el funcionamiento del nuevo sistema SITEL es qué sucede, una vez finalizada la intervención, con las grabaciones y los datos que se han obtenido.

En este punto, encontramos discrepancias importantes en las sentencias de la Sala Segunda. En efecto, en la STS de 13 de marzo de 2009 se hace una descripción del funcionamiento del SITEL, en la que se afirma que finalizada la intervención y una vez se vuelcan todos los datos al formato DVD, se verifica que en la sede central no queda vestigio de la información. También en la STS de 17 de noviembre de 2009 se afirma que el espacio de almacenamiento tiene una gran capacidad y su contenido queda a disposición de la autoridad judicial, que será la competente para ordenar la eliminación del contenido de las grabaciones. En la STS de 12 de noviembre de 2009 se afirma que se conserva el archivo sonoro matriz en el disco duro del servidor central. O, finalmente, en la STS de 23 de marzo de 2009 se afirma que lo que realmente interesa no es lo que pueda suceder con las conversaciones grabadas si quedan bajo el control del Ministerio del Interior o de la autoridad judicial, ya que lo que realmente importa es si se respetaron las debidas garantías en su obtención y su incorporación al proceso y que, en todo caso, determinar el sistema a seguir para conservar o no conservar y controlar las conversaciones legalmente intervenidas y grabadas es un tema que interesa a la Administración y al poder legislativo.

Contrariamente a lo que se expone en esta última resolución, creo que la conservación del resultado de las interceptaciones no es una cuestión irrelevante. Puede serlo a efectos de analizar la regularidad de las conversaciones en el proceso concreto en que se ha realizado la interceptación, pero saber si realmente el contenido de las intervenciones queda almacenado *sine die* en el servidor central tiene una importancia significativa.

Como recalca la reciente STEDH (Sentencia del Tribunal Europeo de Derechos Humanos) de 10 de febrero de 2009, caso Lordachi contra Moldavia, entre las exigencias de regulación suficiente de las intervenciones telefónicas hay que hacer mención especial del procedimiento que se ha de seguir para el examen, el uso y la conservación de la información obtenida, las precauciones que hay que adoptar en la comunicación de la información a las partes y las circunstancias en que las grabaciones pueden ser borradas o las cintas inutilizadas, siempre bajo el control de la autoridad judicial.

## 6. CONCLUSIONES

Lo cierto es que sobre el funcionamiento del sistema SITEL, como ya hemos podido ver y se indica en el voto particular, se ha establecido una minuciosa regulación en todos los aspectos que se refieren al cumplimiento de las órdenes de interceptación y a las garantías que deben rodearlas; pero esta regulación no existe, no sólo por lo que respecta a la transmisión de la información a la autoridad judicial solicitante, sino especialmente por lo que respecta a la custodia y a la conservación de esta información. Pero lo más importante es que no se desprende de manera clara qué sucede con las intervenciones finalizadas. No obstante, cabe pensar que efectivamente se conservan copias de seguridad de los ficheros en el servidor central, como se señala en el BOE núm. 256, de 25 de octubre de 2007, que publica la adjudicación del servicio de mantenimiento del entorno de alta disponibilidad y plataforma de almacenamiento/archivado/*back up* al Sistema de Interceptación de las Telecomunicaciones, ubicado en el complejo policial de Canillas, de manera que ciertamente, como apuntaba, parece que existe esta posibilidad.

Y esta posibilidad nos lleva a cuestiones ciertamente relevantes.

La primera de ellas es obviamente si la autoridad judicial puede acordar la destrucción o la inutilización de la información una vez ha finalizado el procedimiento por resolución firme con responsabilidad penal declarada, o bien cuándo se ha de dictar resolución que finalice el procedimiento sin declaración de responsabilidad penal. Hay que tener en cuenta que la interceptación de las comunicaciones es una medida de carácter exclusivamente jurisdiccional aunque su ejecución material esté a cargo de los cuerpos de seguridad, de manera que una vez ha finalizado la intervención y sus resultados han sido aportados al juzgado de instrucción, su control es estrictamente jurisdiccional; por tanto la autoridad judicial debería poder acordar la inutilización de la información almacenada.

La segunda cuestión que surge es si una vez realizada la intervención en un proceso determinado y finalizado este proceso, la información que en su momento se obtuvo y que queda en el servidor central puede ser utilizada en otra investigación policial.

Lo cierto es que el uso de la información revelada por intervenciones telefónicas acordadas judicialmente en un proceso determinado para otro proceso ha sido admitido por la jurisprudencia de la Sala Segunda, e incluso ha dictado un

Acuerdo de la Sala para determinar las condiciones de impugnación de la prueba aportada en el segundo proceso.

En todo caso, lo que parece evidente es que el acceso a la información que consta archivada debería hacerse en las mismas condiciones y con los mismos requisitos exigibles a la intervención inicial, es decir, autorización judicial con la motivación y los requisitos genéricos de cualquier intervención.