DUES INTERVENCIONS SOBRE INVESTIGACIÓ PENAL I DADES PERSONALS

Aquest article recull de manera conjunta les intervencions de la directora del Centre d'Estudis Jurídics i Formació Especialitzada i de la directora de l'Agència Catalana de Protecció de Dades realitzades en les Jornades sobre Jutges, Fiscals i Policies, vèrtex d'aquest número de la Revista.

Si bé, d'una banda, la intervenció de la primera tracta els punts forts i febles del Sistema Integrat d'Intercepció de les Telecomunicacions (SITEL) pel que fa a la validesa i l'eficàcia de les proves obtingudes mitjançant aquest sistema en el procés penal, la segona aborda la protecció i el tractament de les dades obtingudes durant la investigació penal per part de les forces i els cossos de seguretat.

Encara que el sistema SITEL permet recollir una gran quantitat d'informació mitjançant la intervenció de les comunicacions en temps real, planteja una sèrie d'incerteses respecte al tractament posterior de les dades obtingudes. Aquest tractament, si més no, hauria de respectar sempre els límits imposats per la Llei 15/1999, de 13 de desembre, de protecció de dades personals i la regulació específica aplicable al tractament de dades per part de les forces de seguretat.

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 INTEGRAT D'INTERCEPCIÓ LEGAL DE LES TELECOMUNICACIONS (SITEL)

ROSER BACH I FABREGÓ
Directora del Centre d'Estudis Jurídics i Formació Especialitzada

1. INTRODUCCIÓ

Em referiré en primer terme al Sistema Integrat d'Intercepció de les Telecomunicacions (SITEL), fixant-me especialment en la recepció que s'ha efectuat en la

jurisprudència de la Sala Segona del Tribunal Suprem, perquè en definitiva ens donarà les claus de quins són els problemes més importants que es plantegen en el procés penal, en concret sobre la validesa i l'eficàcia probatòria de les evidències obtingudes a través d'aquest sistema d'intercepció de les comunicacions i de les solucions que es proposen, i també dels problemes que no s'han plantejat i que de ben segur apareixeran.

Va ser als volts de l'any 2000, quan ja hi havia hagut un auge extraordinari en la utilització de la telefonia mòbil i, conseqüentment, de l'ús per part de la delinqüència organitzada, que es va posar de manifest la manca d'operativitat i les dificultats pràctiques per a dur a terme les intervencions telefòniques amb els sistemes d'intercepció tradicionals.

És en aquest marc que el Govern de l'Estat va encarregar a una empresa especialitzada la creació d'un sistema que pogués resoldre aquests problemes d'efectivitat en les intercepcions de les comunicacions.

El que havia de permetre aquest nou sistema era el canvi d'un sistema manual a un sistema digital, la intercepció i l'escolta de les comunicacions en temps real, la capacitat d'emmagatzemar totes les converses fetes a través dels números intervinguts i, al mateix temps, proporcionar una gran quantitat d'informació complementària, com per exemple la identitat i la localització física de les persones interlocutores, l'IMEI[1] dels terminals, els missatges SMS, etc.

Després de diversos intents de posar-lo en marxa, amb una proposta de Reglament, i amb l'aparició de dos informes contraris al nou sistema (Agència Espanyola de Protecció de Dades i el Consell General del Poder Judicial), finalment es va posar en marxa l'any 2004.

Mitjançant el Reial decret 424/2005, de 15 d'abril, es va aprovar el Reglament sobre les condicions per a la prestació de serveis de comunicacions electròniques, el servei universal i la protecció dels usuaris.

Com ja he avançat abans, la recepció en la jurisprudència de la Sala Segona del Tribunal Suprem ens pot donar una idea dels problemes que es plantegen i que es plantejaran en un futur en relació amb aquest sofisticat sistema d'intercepció de les comunicacions, més tenint en compte que finalment caldrà analitzar la valoració com a proves de les dades obtingudes amb la utilització del SITEL, i també tenint en compte que, al meu entendre, hi ha un gran desconeixement a jutjats i tribunals del funcionament real d'aquest nou sistema, malgrat el temps que fa que està implantat.

Els aspectes essencials que es tracten en les resolucions dictades fins al moment són els que exposo en els apartats següents.

1. L'IMEI és l'identificador únic a escala mundial que es dóna a cada terminal d'un sistema de comunicació mòbil. La sigla correspon a la denominació anglesa *international mobile equipment identity* (identificador internacional d'equipament de mòbil) [n. de l'ed.].

2. FUNCIONAMENT OPERATIU DEL SISTEMA SITEL

En la Sentència del Tribunal Suprem (STS) de 13 de març de 2009 es fa una extensa explicació del funcionament del sistema SITEL.

El SITEL és una implementació sobre la qual exerceix la titularitat el Ministeri de l'Interior. El seu desenvolupament respon a la necessitat d'articular un mecanisme modern, automatitzat, simplificador i garantista per a la figura o el concepte de la intervenció de les comunicacions.

El sistema s'articula en tres principis d'actuació:

a) Centralització

El servidor i administrador del sistema es troba a la seu central de la Direcció General de la Policia i la Guàrdia Civil, que distribueix la informació aportada per les operadores de comunicacions als diversos usuaris implicats.

b) Seguretat

El sistema estableix nombrosos filtres de seguretat i responsabilitat, basats en el principi anterior. Hi ha dos nivells de seguretat:

— *Nivell central*

Disposa d'un ordinador central del sistema dotat del màxim nivell de seguretat, amb uns operaris específics de manteniment, on es dirigeix la informació als punts d'accés perifèrics de forma estanca. La missió d'aquest nivell central és emmagatzemar la informació i distribuir-la.

— *Nivell perifèric*

El sistema compta amb ordinadors únics per a aquest ús en els grups perifèrics d'enllaç en les unitats encarregades de la investigació i responsables de la intervenció de la comunicació, dotats d'un sistema de connexió amb la seu central propi i segur. S'estableix una codificació d'accés per a l'usuari autoritzat i una clau personal, que garanteixen la connexió al contingut autoritzat d'informació per a aquest usuari, el qual cal que sigui forçosament component de la unitat d'investigació encarregada i responsable de la intervenció.

c) Automatització

El sistema respon a la necessitat de modernitzar el funcionament de les intervencions de les comunicacions, per dotar-lo d'un nivell més gran de garantia i seguretat, reduir costos i espai d'emmagatzemament, així com per adaptar-se a l'ús de nous dispositius d'emmagatzematge.

La informació relativa a dades telefòniques que en l'actualitat aporta el sistema és la següent:

— data, hora i duració de les trucades
— identificador d'IMEI i número de mòbil afectat per la intervenció
— distribució de les trucades per dia
— tipus d'informació continguda (SMS, carpeta d'àudio, etc.)

Pel que fa al contingut de la intervenció de la comunicació i el tipus d'informació aportada pel sistema, es verifica els punts següents:

— repetidor activat i mapa de la seva situació
— número de telèfon que efectua la trucada o contingut de la informació
— contingut de les carpetes d'àudio (trucades) i dels missatges de text (SMS)

Quant al sistema de treball, un cop s'ha sol·licitat la intervenció de la comunicació i l'autoritat judicial hagi autoritzat l'ús del programa SITEL, l'operadora afectada inicia l'enviament de la informació al servidor central, on s'emmagatzema a disposició de la unitat encarregada i sol·licitant de la investigació dels fets, responsable de la intervenció de la comunicació.

El personal d'aquesta unitat hi accedeix, com s'ha dit més amunt, mitjançant el codi identificador d'usuari i la clau personal. Després de supervisar el contingut, s'actua igual que amb el sistema tradicional, és a dir, s'elaboren les diligències d'informe corresponents per a l'autoritat judicial. L'evidència legal del contingut de la intervenció és aportada pel servidor central, des del qual s'aboquen i enregistren totes les dades en format DVD, que es constitueix com a única versió original. D'aquesta manera l'espai d'emmagatzemament es redueix considerablement, cosa que facilita l'entrega de la unitat d'investigació a l'autoritat judicial competent, i també es verifica que en seu central no hi queda vestigi de la informació.

3. LA NECESSITAT DE PETICIÓ EXPRESSA DE LES INTERVENCIONS MITJANÇANT EL SISTEMA SITEL A L'AUTORITAT JUDICIAL

El SITEL permet un nivell d'intervenció molt superior als sistemes tradicionals, especialment pel que fa al grau d'informació que pot proporcionar. Com hem vist abans, fins i tot és possible la localització física de la persona que efectua la comunicació telefònica.

Aquesta potencialitat informativa determina que per a l'autorització de la intervenció als agents policials encarregats de la investigació cal que la petició sigui especialment detallada en dos sentits.

De fet, la STS de 17 de novembre de 2009 afirma que el SITEL és un mètode avançat i extremadament invasiu de la intimitat, de manera que la petició policial ha d'explicar, encara que sigui sumàriament, quins són els objectius que es pretenen assolir i les conseqüències del funcionament del sistema.

Així doncs, en primer lloc, a més dels requeriments de determinació objectiva i subjectiva que ha establert reiteradament el Tribunal Constitucional, cal que a la sol·licitud policial, en el cas que la intervenció es pretengui dur a terme amb el sistema SITEL, s'assenyali de forma expressa que la intervenció es farà amb aquest sistema —d'altra banda, fet habitual a la pràctica— i, en segon lloc, dins de les àmplies possibilitats que ofereix el sistema pel que fa a dades que es poden obtenir, quin serà en aquest sentit l'abast de la intervenció.

4. L'APORTACIÓ AL JUTJAT D'INSTRUCCIÓ DE LES GRAVACIONS EN FORMAT DVD

Amb els sistemes tradicionals d'intervenció de les comunicacions, una vegada finalitzada la intervenció, les cintes o els suports que contenien les gravacions originals eren aportades al jutjat d'instrucció que havia autoritzat la mesura.

En efecte, la jurisprudència tant del Tribunal Constitucional com del Tribunal Suprem ha exigit que l'aportació de les cintes de les gravacions ha de ser íntegra i original, de manera que —sens perjudici de la selecció que pugui realitzar el jutge instructor o els mateixos policies encarregats de la investigació— el que serà determinant a l'efecte de dotar de valor probatori les converses és que les cintes originals hagin estat entregades al jutjat d'instrucció i estiguin a disposició de les parts.

Es tractava d'un requisit de caràcter processal que no afectava la regularitat de la ingerència en el dret al secret de les comunicacions, però sí a la virtualitat probatòria de les intervencions telefòniques.

Amb aquesta perspectiva canvia substancialment el funcionament del SITEL. En efecte, amb el nou sistema, una vegada acordada la intercepció de les comunicacions, aquesta es realitza de forma automatitzada i se'n fa una gravació també automatitzada en el servidor central; quan finalitza la intervenció s'aboca la gravació a suport DVD, que és el que s'aporta al jutjat d'instrucció.

Per tant, ja no es pot parlar pròpiament de gravacions originals, excepte les que constaran en el disc dur del servidor central, i el que sempre s'ha d'aportar al jutjat d'instrucció és la còpia de la informació abocada en format DVD.

La jurisprudència de la Sala Segona s'ha referit a aquest aspecte en diverses resolucions sobre recursos, en els quals precisament s'impugnava que els agents policials actuants no havien aportat al procediment les gravacions originals, fent referència a l'exigència ja esmentada d'aportar-les amb la tecnologia tradicional.

Per exemple, la STS de 17 de novembre de 2009 indica en relació amb aquesta exigència d'aportació del suport original que, amb el sistema tradicional, mai s'havia exigit el trasllat a la seu judicial del suport que albergava la bobina de les cintes, que seria l'equivalent al disc dur centralitzat amb el nou sistema d'intercepció. Tot i així, crec que la comparació és poc oportuna ja que, sens perjudici del que es consideri que s'ha d'aportar al jutjat d'instrucció, no es pot equiparar la gravació original que es demana amb el suport físic on aquesta es conté.

Aquesta sentència també afegeix, incidint en l'autenticitat de les gravacions, que l'automatització del sistema SITEL no exigeix la presència permanent d'una persona escoltant en temps real les converses intervingudes, ja que amb la nova tecnologia se substitueix aquesta presència personal amb un sistema de gravació d'alta seguretat i de difícil —per no dir impossible— manipulació, sense que la persona que eventualment la fes fos detectada per la seva clau i personalment identificada amb més seguretat que amb un sistema tradicional de cintes analògiques.

Altres sentències de la Sala Segona, com la de 12 de novembre de 2009, argumenten que el disc amb l'arxiu sonor procedent del servidor central certificat digitalment ha de considerar-se arxiu original, amb independència que es conservi l'arxiu sonor matriu en el disc dur del servidor central.

En el mateix sentit, la STS de 13 de març de 2009 afirma que el DVD que conté la gravació de les dades es constitueix com l'única versió original.

En aquest punt cal fer referència al vot particular de la STS d'1 de febrer de 2009. Independentment que es comparteixin o no les afirmacions i, sobretot, les objeccions que es fan en la sentència al sistema SITEL, la seva lectura és interessant perquè també es refereix al valor probatori dels DVD que s'aporten al procediment.

En la sentència majoritària es va desestimar la impugnació dels recurrents en el sentit de qüestionar l'autenticitat dels DVD posats a disposició del jutge d'instrucció que contenen les converses telefòniques de les persones imputades.

Assenyalen els magistrats que subscriuen el vot particular que quan es qüestiona aquesta autenticitat la resposta no pot consistir en un acte de fe inspirat en les excel·lències del software que utilitzen els agents policials, ni tampoc es pot convertir en un debat sobre la credibilitat de les forces i els cossos de seguretat de l'Estat, sinó que afirmen que es tracta d'un problema de caràcter jurídic, específicament processal, sobre el valor atribuïble a aquests suports que constitueixen una prova electrònica. Per tant, es tracta d'una problemàtica aliena a la suficiència tècnica del SITEL i al funcionament del sistema respecte a l'àmbit de la protecció de dades. Es tracta, com s'ha dit, d'un problema processal, del valor probatori atribuïble als DVD que s'incorporen al procés.

El vot particular en primer terme repassa les deficiències regulatives pel que fa al control de l'autenticitat i integritat del document digital i, en segon terme, exposa quins haurien de ser els requeriments del document per satisfer aquestes exigències.

El vot particular fa un repàs dels supòsits en què l'Administració ha implantat la utilització de documents electrònics i els requisits que ha establert en la normativa reguladora corresponent, com per exemple en l'àmbit del notariat, en l'àmbit de l'accés electrònic de la ciutadania al servei públic en l'intent de crear una autèntica administració electrònica, o la documentació electrònica del judici oral; àmbits en els quals el legislador no ha estat aliè a les exigències d'autenticitat i ha establert rigorosos requisits que fan referència essencialment a la signatura electrònica.

Dons bé, remarca el vot particular que, a la vista de la normativa que regula el sistema SITEL, totes aquestes garanties que tendeixen a preservar l'autenticitat i la integritat dels documents digitals només s'han establert en la relació que es produeix entre els agents de policia facultats i les operadores de telefonia. En efecte s'estableixen requisits exigents i formalitats tècniques en el flux d'informació entre els servidors de telefonia i els agents facultats, però tot aquest sistema de garanties desapareix quan els agents facultats aboquen en un DVD les converses que estimen rellevants i el presenten al jutjat.

Continua el vot particular indicant que la implantació d'un sistema que ofereix tantes possibilitats com el SITEL no hauria d'haver prescindit d'una idea tan elemental com l'existència de tres subjectes funcionals diferents:

a) les operadores de telefonia (subjectes obligats),
b) els funcionaris de policia (agents facultats),
c) els jutges d'instrucció que autoritzen la intercepció i es converteixen en els destinataris últims del resultat de les escoltes.

I afirma que d'aquesta manera el SITEL converteix els jutjats i tribunals en «un punt feble», en «una terra de ningú» en la qual les garanties de seguretat i integritat del document electrònic es degraden de forma insalvable; igualment, afirma el vot particular, els jutges d'instrucció es converteixen en simples receptors d'uns suports electrònics el contingut dels quals no es pot basar en cap altra garantia que no sigui la confiança acrítica en la professionalitat dels agents que els els proporcionen. De la mateixa manera, el secretari judicial, en la seva condició de fedatari, es veu obligat a subscriure un acte d'asseveració a cegues, no pot donar fe que el contingut dels DVD coincideix amb l'original al qual no té accés, ja que l'oficina judicial no pot fer un seguiment de les intercepcions.

Una vegada exposades les deficiències en la regulació del sistema, el vot particular detalla els requisits que haurien de complir els documents digitals en què s'incorporen les gravacions, que evidentment —indiquen— constitueix prova electrònica.

Pel que fa a l'anàlisi de l'autenticitat, els magistrats destaquen que cal exigir dos nivells d'autenticitat. En primer lloc el que garanteix que, un cop gravada la conversa en el terminal custodiat pels agents de policia, el fitxer generat no ha estat obert amb posterioritat i per tant no ha estat exposat a cap mena de modificació. El segon nivell deriva del fet que la prova que s'ofereix al tribunal està integrada no pels ordinadors centrals sinó per còpies incorporades a un o més DVD, de manera que aquest nivell d'autenticitat consisteix a assegurar que, immediatament després de finalitzat el procés de gravació, s'activi una certificació que garanteixi que:

a) des del moment en què s'acaba el procés de gravació fins que la rep el jutjat el DVD no ha estat obert;
b) en conseqüència no ha existit risc de manipulació, i
c) qui garanteix la integritat del document és el funcionari responsable del tractament i, per tant, l'únic amb capacitat d'autentificació.

Això no obstant, els magistrats discrepants reiteren que aquestes mesures de seguretat no s'han previst, de manera que el compliment d'aquestes exigències és realment complicat.

En aquest punt, penso que es pot concloure que en el disseny del sistema s'hauria d'haver previst la possibilitat —que tècnicament segur que és factible— que l'òrgan judicial pogués tenir accés al servidor central, que és on efectivament s'allotja la gravació original, o, si s'escau, a una certificació digital d'integritat i autenticitat; de tal manera que el secretari judicial estigués en condicions de certificar la correlació del DVD entregat al jutjat d'instrucció amb la versió original, com es feia tradicionalment amb el sistema ordinari d'intervenció.

5. LA CONSERVACIÓ DE LES INTERVENCIONS I LES DADES OBTINGUDES

Una de les qüestions que adquireix una importància significativa en el funcionament del nou sistema SITEL és què succeeix, una vegada finalitzada la intervenció, amb les gravacions i les dades que s'han obtingut.

En aquest punt a les sentències de la Sala Segona trobem discrepàncies importants. En efecte, a la STS de 13 de març de 2009 es fa una descripció del funcionament del SITEL, en què s'afirma que finalitzada la intervenció i una vegada s'aboquen totes les dades a format DVD, es verifica que en seu central no hi queda cap vestigi de la informació. També a la STS de 17 de novembre de 2009 s'afirma que l'espai d'emmagatzemament té una gran capacitat i el seu contingut queda a disposició de l'autoritat judicial, que serà la competent per a ordenar l'eliminació del contingut de les gravacions. A la STS de 12 de novembre de 2009 s'afirma que es conserva l'arxiu sonor matriu en el disc dur del servidor central. O, finalment, a la STS de 23 de març de 2009 s'addueix que el que interessa no és el que pugui succeir amb les converses gravades si queden sota el control del Ministeri de l'Interior o de l'autoritat judicial, ja que el que realment importa és si es van respectar les degudes garanties en la seva obtenció i la seva incorporació al procés, i que en tot cas concerneix l'Administració i el poder legislatiu determinar el sistema a seguir per a conservar o no conservar i controlar les converses legalment intervingudes i gravades.

Contràriament al que s'exposa en aquesta darrera resolució, crec que la conservació del resultat de les intercepcions no és una qüestió irrellevant. Pot ser-ho a l'efecte d'analitzar la regularitat de les converses en el procés concret en què la intercepció s'ha realitzat, però té una importància significativa conèixer si realment el contingut de les intervencions resta *sine die* emmagatzemat al servidor central.

Com recalca la recent STEDH (Sentència del Tribunal Europeu de Drets Humans) de 10 de febrer de 2009, cas Lordachi contra Moldavia, entre les exigències de regulació suficient de les intervencions telefòniques cal fer especial esment del procediment que s'ha de seguir per a l'examen, l'ús i la conservació de la informació obtinguda, les precaucions que cal adoptar en la comunicació de la informació a les parts i les circumstàncies en què les gravacions poden ser esborrades o les cintes inutilitzades, sempre sota el control de l'autoritat judicial.

6. CONCLUSIONS

El cert és que sobre el funcionament del sistema SITEL, com ja hem pogut veure i s'indica en el vot particular, s'ha establert una regulació minuciosa en tots els aspectes que es refereixen a compliment de les ordres d'intercepció i a les garanties que l'han de rodejar; però aquesta regulació no existeix, no només pel que fa a la transmissió de la informació a l'autoritat judicial sol·licitant, sinó especialment pel que fa a la custòdia i la conservació d'aquesta informació. Però el més important és que no se'n desprèn de manera clara què succeeix amb les intervencions finalitzades. Això no obstant, es pot pensar que efectivament es conserven còpies de seguretat de fitxers en el servidor central (el BOE núm. 256, de 25 d'octubre de 2007, publica l'adjudicació del servei de manteniment de l'entorn d'alta disponibilitat i plataforma d'emmagatzemament/arxivat/*back up* del Sistema d'Intercepció de les Telecomunicacions), ubicat en el complex policial de Canillas, de manera que certament, com apuntava, sembla que hi ha aquesta possibilitat.

I aquesta possibilitat ens porta a qüestions certament rellevants.

La primera d'elles és òbviament si l'autoritat judicial pot acordar la destrucció o la inutilització de la informació una vegada ha finalitzat el procediment per resolució ferma amb responsabilitat penal declarada, o bé quan s'ha dictar resolució que finalitza el procediment sense declaració de responsabilitat penal. Cal tenir en compte que la intercepció de les comunicacions és una mesura de caràcter exclusivament jurisdiccional encara que la seva execució material estigui a càrrec dels cossos de seguretat, de manera que una vegada ha finalitzat la intervenció i els seus resultats han estat aportats al jutjat d'instrucció, el seu control és estrictament jurisdiccional, per tant l'autoritat judicial hauria de poder acordar la inutilització de la informació emmagatzemada.

La segona qüestió que sorgeix és si un cop realitzada la intervenció en un procés determinat i finalitzat aquest procés, la informació que en el seu moment es va obtenir i que resta en el servidor central pot ser utilitzada en una altra investigació policial.

El cert és que l'ús de la informació revelada per intervencions telefòniques acordades judicialment en un procés determinat per a un altre procés ha estat admès per la jurisprudència de la Sala Segona, i fins i tot ha dictat un Acord de la Sala per a determinar les condicions d'impugnació de la prova aportada al segon procés.

En tot cas, el que sembla evident és que l'accés a la informació que consta arxivada s'haurà de fer en les mateixes condicions i amb els mateixos requisits exigibles a la intervenció inicial, és a dir, mitjançant una autorització judicial amb la motivació i els requisits genèrics de qualsevol intervenció.