

TRIBUNAL SUPREMO

Sala de lo Penal

VOTO PARTICULAR

FECHA:01/02/2010

VOTO PARTICULAR QUE FORMULA EL EXCMO. SR. D. MANUEL MARCHENA GÓMEZ, EN LA SENTENCIA RECAÍDA EN EL RECURSO DE CASACIÓN NÚM. 404/2009, AL QUE SE ADHIERE EL EXCMO. SR. D. JOSÉ MANUEL MAZA MARTÍN.

I.- Mediante el presente voto particular queremos expresar nuestro desacuerdo con el criterio de nuestros compañeros acerca de las garantías de autenticidad exigibles a los DVDs puestos a disposición del Juez instructor por los agentes de policía, en los que se contienen las conversaciones telefónicas de los imputados.

A nuestro juicio, la atribución de eficacia probatoria a esos DVDs ñexpresamente impugnados en su autenticidad por la defensa de uno de los recurrentes-, supone un retroceso respecto del estado actual de las garantías constitucionales (arts. 18.3 y 24.2 CE). Y esa relajación del nivel de exigencia que esta Sala y la jurisprudencia constitucional han venido imponiendo, se produce en una materia ñla prueba electrónica- caracterizada precisamente por su volatilidad y las infinitas posibilidades de manipulación y tratamiento.

Cuando se nos pide un pronunciamiento acerca de la cuestionada autenticidad de unos DVDs -en este caso, ofrecidos por la Policía- nuestra respuesta no puede consistir en un acto de fe inspirado por las excelencias del *software* del que se valen los agentes. Tampoco podemos incorporar al objeto del debate el grado de confianza institucional que a la Sala le merezca el trabajo de las Fuerzas y Cuerpos de Seguridad del Estado. Algunos pasajes de la sentencia (óë *la autenticidad del contenido de los discos está fuera de discusión. Si en alguna ocasión las*

partes personadas estiman que los discos depositarios de la grabación no responden a la realidad, deberán explicar suficientemente en qué basan su sospecha en cuanto que están acusando de un hecho delictivo a los funcionarios que se encargan del control del sistema SITEL®) desenfocan el núcleo del problema, convirtiendo lo que debería ser un debate genuinamente jurídico en un juicio sobre la credibilidad que nos inspira la labor de las Fuerzas y Cuerpos de Seguridad del Estado.

Y no es esto lo que está en juego.

El enunciado del problema es mucho más sencillo. Lo que se requiere de nosotros no es que avalemos la suficiencia técnica del procedimiento mediante el que se graban las conversaciones intervenidas. Tampoco que examinemos el funcionamiento del sistema con la perspectiva de su validez en el ámbito de la protección de datos personales. Nuestro razonamiento, por el contrario, no puede tener otro objetivo que dar respuesta, en el plano estrictamente jurídico, a un problema procesal, esto es, al valor probatorio atribuible, desde la perspectiva de su autenticidad, a la prueba electrónica.

Que los DVDs ofrecidos por los agentes de policía constituyen una prueba electrónica es algo que está fuera de dudas. Sin entrar en la controversia doctrinal, de especial interés en el proceso civil, acerca de si esos DVDs merecerían el tratamiento de una verdadera prueba documental (art. 317 LECiv) o, por el contrario, de una prueba autónoma, de significado diferente (art. 382 LECiv), lo que resulta incuestionable es que su valoración probatoria ha de ajustarse a las reglas generales.

A nuestro juicio, si bien la fuerza probatoria de los documentos electrónicos no tiene por qué ser cuestionada *a priori*, en aquellos casos en los que se impugne su exactitud e integridad en momento procesal oportuno ñy el escrito de conclusiones provisionales, desde luego, lo es-, surge en la acusación el deber de desplegar un esfuerzo probatorio que acredite, sin perjuicio de las dificultades inherentes a una prueba pericial sobre esta materia, que esa objeción de la defensa no resulta justificada.

Esta idea tan elemental es congruente con el contenido del art. 230 de la LOPJ, con arreglo al cual, los Juzgados y Tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones, añadiendo que *óë los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales*ô.

En numerosos precedentes, referidos a los soportes convencionales de las escuchas telefónicas, hemos afirmado que sólo cuando se impugne la autenticidad de las grabaciones, será necesario acudir a medios de prueba adicionales que acrediten la misma (cfr., por todas, SSTS 1075/2004, 24 de septiembre y 1566/2005, 30 de diciembre), precisando incluso que la convicción sobre la autenticidad de las voces no precisa apoyarse, como presupuesto constitutivo de validez, en una prueba pericial (STS 593/2009, 8 de junio).

Sin embargo, desde la perspectiva de los soportes electrónicos actuales, cuando la impugnación se refiere, no a la *atribuibilidad* de las voces recogidas en la grabación, sino al procedimiento técnico llamado a asegurar la integridad y autenticidad de tales soportes, la necesidad de despejar cualquier duda sobre las garantías de sellado de los archivos de voz, adquiere un significado especial.

Anticipamos nuestro criterio de que no existen razones jurídicas que justifiquen que el resultado de los actos de investigación encomendados a las Fuerzas y Cuerpos de Seguridad del Estado se sustraigan a las reglas generales sobre la valoración de la autenticidad de un documento electrónico. En nuestra opinión, los DVDs aportados a un proceso penal por agentes de policía no pueden aspirar a un régimen privilegiado frente a la autenticidad afirmable de esos mismos soportes electrónicos cuando tienen distinto origen.

Dicho con otras palabras, el DVD aportado por los agentes no puede gozar de una autenticidad, irrazonablemente aventajada, frente al DVD en el que se contienen, por ejemplo, escrituras públicas y está

custodiado por un Notario. Por la misma razón, carece de sentido que las garantías que el Ministerio de Justicia ha impuesto en el diseño de la remozada oficina judicial o en la creación del nuevo Registro electrónico, y las exigencias que el Ministerio de Hacienda define a la hora de aceptar las declaraciones tributarias por vía telemática, se difuminen hasta desaparecer cuando de lo que se trata es de ofrecer al Juez de instrucción unos DVDs que contienen cientos de horas de conversaciones telefónicas que, en la mayoría de los casos, se convierten en el respaldo decisivo de una condena penal.

Somos conscientes de que la garantía que proporciona la firma electrónica sólo alcanza a algunos de los aspectos ligados a la incolumidad y a la identificación del firmante que está en el origen de los archivos incorporados al soporte electrónico (art. 3 de la Ley 59/2003, 19 de diciembre). Precisamente por ello, en el apartado IV de este voto particular, razonamos acerca de los presupuestos indispensables para que aquellos soportes probatorios, más allá de la garantía que aporta la firma electrónica, superen el verdadero *test de admisibilidad*. Pese a todo, nos interesa destacar, con breve cita de algunos preceptos de nuestro ordenamiento jurídico, cómo la afirmación que hace la sentencia, referida a una supuesta *presunción de autenticidad* de los DVDs, carece de cobertura en nuestro sistema.

II.- El art. 115 de la Ley 24/2001, 27 de diciembre, dio nueva redacción al art. 17 bis de la más que centenaria Ley del Notariado, fechada el 28 de mayo de 1862. En su apartado 3 se regula la garantía que ha de reunir una copia notarial para estimar acreditada su autenticidad. En él se dispone: *óë las copias autorizadas de las matrices podrán expedirse y remitirse electrónicamente, con firma electrónica avanzada, por el notario autorizante de la matriz o por quien le sustituya legalmenteô*.

Pero las garantías asociadas a los archivos y documentos electrónicos, no son exclusivas del trabajo desplegado por los Notarios. La propia Administración impone semejantes requerimientos técnicos de autenticidad cuando es el ciudadano el que se relaciona con los órganos administrativos.

En efecto, la *Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos*, ha querido definir las condiciones para que la actividad administrativa y las relaciones de los poderes públicos con los ciudadanos puedan ajustarse a las nuevas tecnologías. Ese ambicioso proyecto, orientado a la creación de una genuina *Administración Electrónica*, no ha pasado por alto las exigencias de autenticidad.

Así, en su art. 13, bajo el epígrafe *formas de identificación y autenticación*, se establece un principio general, referido a la admisibilidad de sistemas de firma electrónica, que luego es objeto de concreción. En el apartado 1 de ese precepto, se dispone que *“las Administraciones Públicas admitirán, en sus relaciones por medios electrónicos, sistemas de firma electrónica que sean conformes a lo establecido en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica y resulten adecuados para garantizar la identificación de los participantes y, en su caso, la autenticidad e integridad de los documentos electrónicos”*.

Añade el apartado 2 que *“los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine: a) en todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas; b) sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas; c) otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen”*.

Definidas las garantías de autenticidad exigibles a los ciudadanos, el mismo precepto, en su apartado 3, se refiere a idéntico tema desde la perspectiva de la propia Administración. En él puede leerse: *“las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan: a) sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de*

comunicaciones seguras; b) sistemas de firma electrónica para la actuación administrativa automatizada; c) Firma electrónica del personal al servicio de las Administraciones Públicas; d) Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

Estas garantías han sido objeto de desarrollo en el Real Decreto 1671/2009, 6 de noviembre, cuyo preámbulo recuerda que, en materia de identificación y autenticación, se impone como medio universal la utilización de dispositivos de firma electrónica, sin perjuicio de otros medios de autenticación que cumplan con las condiciones seguridad y certeza necesarias.

Es comprensible que el Ministerio de Justicia no haya permanecido al margen de esa preocupación legislativa tendente a asegurar la autenticidad de los ficheros electrónicos. Así se desprende, por ejemplo, de la *Orden Ministerial 3000/2009, 29 de octubre, por la que se crea y regula el Registro Electrónico del Ministerio de Justicia*. En su art. 9.1 se dispone que *“los escritos, solicitudes y comunicaciones remitidos por medios electrónicos exigirán la identificación de los interesados remitentes y podrán firmarse mediante: a) los sistemas de identificación y firma electrónica incorporados al documento nacional de identidad para personas físicas; b) los sistemas de firma electrónica avanzada y firma electrónica reconocida; c) las claves concertadas previo registro como usuario, la información conocida por ambas partes u otros sistemas no criptográficos, en los términos que especifiquen las instrucciones de acceso y utilización del Registro Electrónico en cada procedimiento disponible en la sede electrónica del departamento”*.

El legislador, hace apenas dos meses, ha abordado la regulación de la documentación de los debates del juicio oral. Lo ha hecho con ocasión de la promulgación de la Ley 13/2009, 3 de noviembre, de reforma de la legislación procesal para la implantación de la nueva Oficina judicial. Y ha proyectado sus previsiones sobre todos los órdenes jurisdiccionales (cfr. arts. 453 de la LOPJ, 743 LECrim, 147 Ley de Enjuiciamiento Civil, 89.2 Ley de Procedimiento Laboral y 63.4 Ley de Jurisdicción Contencioso-administrativa).

La filosofía que inspira la reforma, en este concreto aspecto, guarda un saludable equilibrio entre el deseo político de implantación de nuevos modelos de gestión procesal y el realismo que impone el desfase tecnológico de nuestros Juzgados y Tribunales. Precisamente por ello, ha impuesto el deber de grabación de las sesiones del juicio oral en un soporte técnico que sea apto para la reproducción del sonido y la imagen. Al mismo tiempo, ha recordado el deber de custodia que incumbe al Secretario judicial respecto de esos soportes. La norma abre la puerta a la utilización de documentos electrónicos cuyo contenido pueda ser adverbado mediante firma electrónica. De su utilización que, como es lógico, estará condicionada a su efectiva disponibilidad en la oficina judicial, se hace depender, tanto la necesidad de presencia real del Secretario judicial en las sesiones del juicio, como las menciones que ha de recoger el acta. La razón es bien clara y se desprende del mismo precepto: sólo en el caso en que el documento esté garantizado con firma electrónica estará a salvo su integridad y autenticidad. Repárese, además, que en el presente caso de lo que se trata es de un documento al que se incorpora un archivo de sonido o imagen que ha sido generado durante el transcurso de un acto procesal, presidido por un órgano jurisdiccional y con la garantía añadida de la custodia formal del fedatario judicial.

En definitiva, el establecimiento de un sistema que garantice, cuando menos, la integridad de cualquier documento electrónico, constituye un *prius* para la atribución al mismo de plena eficacia probatoria. Así lo ha entendido el legislador español -en sintonía con un imparable proceso de unificación en el ámbito de la Unión Europea-, requiriendo esas garantías incluso cuando el documento emana de un fedatario público.

III.- Las normas jurídicas que regulan el funcionamiento del sistema integrado de interceptación telefónica son básicamente dos. Una de ellas, el Real Decreto 424/2005, 15 de abril, buena parte de cuyo contenido fue incorporado al art. 33 de la Ley 32/2003, 3 de noviembre, General de las Comunicaciones, en virtud de la reforma operada por la Disposición Final 1ª de la Ley 25/2007, 18 de octubre, sobre conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Esta norma ha de ser completada con la Orden ITC/110/2009, 28 de enero, por la que se determinan los requisitos y las especificaciones técnicas que resultan necesarios para el desarrollo del Capítulo II del Título V del Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real Decreto 424/2005, 15 de abril.

Pues bien, la lectura detenida de ambos textos normativos -en especial, de este último, que fija los requerimientos técnicos exigibles para la ejecución de la orden judicial de interceptación-, pone de manifiesto que todas las garantías y reservas que el sistema incorpora, sólo miran a la relación entre los agentes de policía facultados y las operadoras de telefonía. La citada OM 110/2009, contempla la necesidad de crear lo que denomina *“bloques funcionales o interfaces del sistema de interceptación legal”*, arbitra varios canales seguros y resuelve los niveles de seguridad exigibles en la dirección bilateral que ha de establecerse entre la Policía y las operadoras para la gestión de la orden judicial de injerencia. El problema radica en que todo ese sistema de controles y garantías se arrincona cuando los agentes facultados vuelcan en un DVD las conversaciones que estiman más relevantes y se presentan ante el Juzgado, mediante una comparecencia personal, aportando un soporte electrónico con vocación de *originalidad*. Éste es el problema de origen que nos impide avalar el funcionamiento del sistema integrado (SITEL) que, si bien se mira, no lleva su *vocación integradora* hasta sus últimas consecuencias, pues se olvida de integrar a los órganos jurisdiccionales en el esquema que define su funcionamiento.

No dudamos de las garantías que el sistema implementa a la hora de asegurar la relación entre los agentes de Policía y los proveedores de telefonía. De hecho, la norma reguladora de los aspectos técnicos derivados de la ejecución de la orden judicial de interceptación telefónica, no desatiende las exigencias de autenticidad en las relaciones entre las Fuerzas y Cuerpos de Seguridad del Estado y las operadoras. En efecto, la ya repetida OM 110/2009, regula de forma casuística las formalidades técnicas que han de reunir los canales de interfaz que hagan posible el flujo de información entre los servidores de telefonía y los agentes facultados. Incluso, la transmisión de información entre ambos ha de realizarse mediante lo que el propio texto denomina *canal seguro electrónico H11* y

valiéndose, como no podía ser de otra manera, de firma electrónica (cfr. Art. 7.2, en relación con los arts. 6 y 8).

Este último dato, por cierto, nos debe hacer pensar en la paradoja que encierra el hecho de que la transmisión de información entre los operadores de telefonía y los agentes facultados de las Fuerzas y Cuerpos de Seguridad del Estado, se verifique con la exigencia de firma electrónica. Sin embargo, en el momento decisivo de su incorporación al proceso penal, para su valoración como fuente de prueba, la relación del órgano jurisdiccional con esos mismos agentes, recupera el añejo sabor artesanal de las comparecencias personales, aportando un documento cuyo contenido ha de ser acatado sin cuestionar su integridad.

La interceptación de las comunicaciones telefónicas con arreglo a las sofisticadas posibilidades que ofrece cualquier sistema integrado, no debería haber prescindido de una idea tan elemental como la existencia de tres sujetos funcionales distintos: a) las operadoras de telefonía *ñsujetos obligados-*; b) los funcionarios de policía *ñagentes facultados-*; c) los Jueces de instrucción que autorizan la interceptación y que se convierten en destinatarios últimos del resultado de las escuchas.

Pues bien, las normas reguladoras del SITEL han diseñado un sistema de garantías en las relaciones entre dos de aquellos sujetos, operadoras y policía. Y lo han hecho cuidando, en ese exclusivo ámbito bidireccional, el espacio que es propio de la intimidad y protección de datos. Sin embargo, todo ello se desmorona de forma incomprensible en el momento de la incorporación de las pruebas electrónicas generadas al proceso penal. En ese instante, los canales seguros y las interfaces que la Orden ITC/110/2009 impone a operadoras y agentes facultados, dejan paso a un incontrolado volcado de datos que, lejos de ser transmitidos por vía telemática, se presentan ante el Juzgado de instrucción por un agente de policía que afirma haber seleccionado aquellos fragmentos que considera relevantes para la investigación.

La preocupación por una seguridad integral, que no admita grietas en alguno de los pilares sobre los que opera el sistema, está bien presente en la Exposición de Motivos del Real Decreto 3/2010, 8 de enero, por el que se regula el *Esquema Nacional de Seguridad en el ámbito de la*

Administración Electrónica. La limitación de su ámbito aplicativo no resta valor a algunos de los pasajes de la Exposición de Motivos. Ahí puede leerse que *“la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse efectivamente para evitar <tierras de nadie> y fracturas que pudieran dañar a la información o a los servicios prestados”*. Insiste el texto en la necesidad de huir de una concepción parcelada y fragmentaria de la seguridad informática: *“se concibe la seguridad como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas”*.

El SITEL, en fin, 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. Los Jueces de instrucción se transforman así en meros receptores de unos soportes electrónicos cuyo contenido no puede apoyarse en otra garantía que la confianza acrítica en la profesionalidad de los agentes que se los proporcionan.

Tal sistema de operar provoca que el Secretario judicial, en su condición de fedatario, se vea obligado a suscribir un acto de adveración a ciegas. No puede dar fe de que el contenido de esos DVDs coincide con un original al que no tiene acceso, pues la oficina judicial ha sido excluida de cualquier interfaz que permita el seguimiento de las interceptaciones. No puede garantizar que no se han eliminado erróneamente fragmentos de conversaciones de indudable trascendencia jurídica y que, sin embargo, han podido ser excluidos en el momento del volcado al soporte electrónico. Dicho de forma bien gráfica, el Secretario sólo podrá advenir que el DVD presentado por la Policía es efectivamente el que presenta la Policía.

De ahí que no podamos compartir el criterio mayoritario, expresado en el FJ 17 de nuestra sentencia, cuando sostiene que *“el sistema de escuchas telefónicas, que se plasma en un documento oficial obtenido con autorización judicial y auténticado su contenido por la fe*

pública judicial goza de valor probatorio, salvo que mediante pericia contradictoria se demuestre la falsedad o alteración de las conversaciones grabadas.

IV.- En nuestra opinión, los soportes digitales aportados por los agentes, como toda prueba electrónica, han de pasar por un *test de admisibilidad*. Y éste comprende el análisis de su integridad, esto es, que el soporte no ha sido alterado; de su autenticidad, o sea, la identificación del sujeto al que se atribuyen las conversaciones y del contenido que éstas reflejan; por último, de su licitud, es decir, de que han sido obtenidos con respeto a los derechos y libertades fundamentales.

En el caso que nos ocupa, a la vista de los términos que definen el objeto del recurso, son los dos primeros aspectos los que han de centrar nuestra atención.

En efecto, la valoración jurisdiccional de un documento electrónico ñen este caso, varios DVDs en los que se incorporan archivos digitales de sonido- exige, a nuestro juicio, dos niveles de autenticidad.

Primero, el que garantiza que, una vez grabada la conversación en el terminal custodiado por los agentes de policía, el fichero así generado no ha sido abierto con posterioridad y, en consecuencia, no ha sido expuesto a ningún tipo de modificación. El Tribunal que ha de valorar esa fuente probatoria ha de tener asegurado, en el plano tecnológico, que no se han suprimido fragmentos relevantes para conocer el alcance de los hechos o que no han sido excluidas conversaciones que el agente responsable considera intrascendentes jurídicamente y que, sin embargo, pueden no serlo. En definitiva, resulta indispensable que el sistema garantice que después de cada conversación interceptada por los agentes facultados se procede al *sellado tecnológico* del archivo de sonido, con el fin de salvaguardar su integridad, excluyendo cualquier riesgo de manipulación. Si, como es lógico y previsible, esos archivos han de ser abiertos durante el desarrollo de la investigación, el sistema podría completarse con la intervención de un tercero ajeno al agente responsable, que encontrara inspiración en los términos del art. 25 de la *Ley 34/2002, 11 de julio, de Servicios de la Sociedad de Información y del Comercio Electrónico*, sin descartar la posibilidad de que ese *sellado*

podiera verificarse a través de una interfaz que conectara al Secretario Judicial con el centro de operaciones, garantizándose así una matriz de prueba frente a posibles y futuras impugnaciones.

Pero no basta con la garantía de que los archivos custodiados en el terminal central no han sido abiertos y, en consecuencia, expuestos a su alteración. Conviene tener presente que la fuente de prueba ofrecida por los agentes de policía a la valoración del Tribunal está integrada, no por los ordenadores centrales, sino por las copias incorporadas a uno o varios DVDs. Se impone, en consecuencia, un segundo nivel de exigencia, que ahora afecta al soporte en el que se incorpora la copia de los archivos originales. De ahí que resulte indispensable que, inmediatamente después de efectuado el proceso de grabación, se active una certificación que garantice: a) que desde el momento en que culminó el proceso de transferencia de archivos hasta su recepción por el Juzgado, ese DVD no ha sido abierto; b) que, en consecuencia, no ha existido riesgo de manipulación; y c) que quien garantiza la integridad del documento es el funcionario responsable del tratamiento y, por tanto, el único con capacidad de autenticación.

Sin embargo, el olvido en el que se ha incurrido a la hora de reglar las medidas de seguridad y autenticidad en la relación del Juez de instrucción con los agentes facultados, complica enormemente nuestro análisis. La normativa vigente reduce las implicaciones jurídicas de una relación trimembre ñórgano jurisdiccional, agentes facultados, operadoras de telefonía-, a un problema a dos, en el que las exigencias de seguridad y autenticidad sólo actúan en la dirección bilateral que afecta a la Policía y a los proveedores de servicio, excluyendo del problema al Juez de instrucción o al Secretario Judicial. No es que los niveles de seguridad se relajen. El problema estriba en que no existen. Ni pocos ni muchos, absolutamente ninguno. No hay interfaz que permita el envío de esos documentos al Juzgado de instrucción por vía telemática y mediante canal seguro. La secuencia grabación-copia-incorporación al proceso se culmina con una simple comparecencia personal, sin filtro alguno que garantice la integridad y autenticidad de los soportes

Este dato, a nuestro juicio, es obviado por el criterio de la mayoría, que concluye la autenticidad de los DVDs a partir de un análisis

incompleto de lo que deben ser las exigencias de seguridad e integridad. Enfatizar que el acceso por parte del personal de la unidad de policía se realiza *óë mediante identificador de usuario y clave personalô*, no añade nada a la solución del problema que nos ocupa. En efecto, esta idea, desarrollada en el razonamiento incorporado al FJ 14, obliga a una importante puntualización. En él puede leerse: *óë se ha dicho que estos discos, dadas las características de la tecnología digital, pueden ser alterados mediante sofisticadas operaciones de laboratorio. Esta objeción no se descarta, ahora bien, así como en el antiguo sistema de manipulación, los cortes eran posibles sin saber de forma cierta quién los había realizado materialmente, en el sistema SITEL se deja huella identificadora del manipulador ya que debe facilitar su clave de identificación para entrar en el disco duro. En este caso, nos encontraríamos ante un delito que de confirmarse su existencia a posteriori podría dar lugar a la revisión de la sentenciaô*.

En nuestra opinión, el control jurisdiccional de las garantías procesales no puede contentarse con la tranquilidad que proporciona que, de producirse una manipulación, la impunidad no estaría garantizada, o con la idea de que siempre habrá tiempo para un ulterior juicio de revisión. Las garantías deben ser inmanentes al sistema, sin que su afirmación pueda quedar postergada a un momento ulterior, una vez detectada su vulneración.

Una cosa es el funcionamiento del SITEL desde la perspectiva de las garantías generales impuestas por nuestro sistema jurídico para la confidencialidad y la protección de datos, cuyo examen y fiscalización corresponde a otras instituciones públicas -cfr. art. 3 del Real Decreto 428/1993, 26 de marzo, por el que se regula el Estatuto de la Agencia de Protección de Datos, art. 22 de la Ley 15/1999, 13 de diciembre, art. 81.1.b) del Real Decreto 1720/2007, 21 de diciembre y Orden INT/1751/2002, 20 de junio, por la que se regulan los ficheros informáticos de la Dirección General de Policía que contienen datos personales-, y otra bien distinta la autenticidad de un soporte informático cuya integridad no ha sido acreditada mediante los medios que el ordenamiento jurídico exige con carácter general. Y es esta segunda cuestión la que constituye el objeto del presente recurso.

El criterio de la mayoría rechaza lo que considera una genérica impugnación de la autenticidad de los DVDs y reprocha al recurrente que no detalle ni explique cuál es el motivo de su oposición. Desde nuestro punto de vista, sin embargo, tal razonamiento está operando como si aquellos soportes contaran a su favor con una presunción de autenticidad de la que, desde luego, carecen.

Por cuanto antecede, entendemos que la impugnación, oportunamente formulada por una de las partes recurrentes, debería haber obligado al Ministerio Fiscal a asegurar, mediante cualquier prueba complementaria, la integridad y autenticidad de esos ficheros. La ausencia de esa actividad probatoria nos lleva a concluir que el motivo que cuestiona la virtualidad probatoria de los DVDs en los que se recogían las conversaciones mantenidas por los imputados, debería haber sido estimado.

Manuel Marchena Gómez

José Manuel Maza Martín

PUBLICACION.- Leída y publicada ha sido la anterior sentencia por el Magistrado Ponente Excmo.Sr. D. José Antonio Martín Pallín, estando celebrando audiencia pública en el día de su fecha la Sala Segunda del Tribunal Supremo, de lo que como Secretario certifico.