

Valor procesal de la prueba informática

José-Ernesto Fernández Pinós

Fiscal Coordinador del Servei Especial de Noves Tecnologies de la Fiscalia del Tribunal Superior de Justícia de Catalunya

¿Qué es una prueba? Desde el punto de vista material, prueba es el indicio, señal o muestra que se da de una cosa, pero desde el punto de vista formal, es la razón o argumento con el que se pretende demostrar la verdad o falsedad de algo. Ambas acepciones son correctas en Derecho, puesto que las partes pretenden acreditar la certeza y validez de sus pretensiones mostrando al tribunal una serie de conjeturas que se apoyan en demostraciones más o menos exactas de lo ocurrido, avaladas por el testimonio de quien presenció los hechos, del documento por el que se formalizó o de los conocimientos del experto que examinó científicamente los indicios. En cierto modo, un juicio es bastante parecido a un mercado, donde las partes muestran y ofrecen sus productos al juez, e intentan convencerle de la idoneidad del mismo frente al producto del puesto de enfrente, bien enseñando la manzana para que pueda apreciar lo lustrosa de su piel (pero procurando siempre tapar esa maca tan poco estética), bien presentándole al experto recolector de manzanas que jurara y perjurara que esa manzana en concreto es la mejor que en el mundo ha existido desde que Eva le ofreció a Adán el fruto del árbol de la Ciencia del Bien y del Mal, bien entregándole el certificado correspondiente a la crianza y conservación de la manzana que, por supuesto, se ha efectuado en las mejores condiciones posibles. Y por si sirve de algo, le dirá que la manzana del vecino no se la comería ni el más hambriento de los hombres, que ha sido cosechada de la peor manera posible y que está repleta de fosfatos, insecticidas y demás sustancias perjudiciales.

En Derecho y como regla general, se puede afirmar que sólo tienen la consideración de pruebas aquellas que se han practicado en el acto del Juicio oral. Es en esta fase procesal cuando tiene lugar la prueba, pues es en ese preciso momento cuando las pruebas se practican con plena observancia de los principios de publicidad, oralidad, inmediación y contradicción, y con el debido respeto a los derechos fundamentales del inculpado a no declarar contra sí mismo y a no confesarse culpable (art. 24.2 CE). No obstante ello, la regla general de que la prueba en el proceso penal únicamente tiene lugar en la fase del Juicio Oral admite diversas excepciones, como son los supuestos de Prueba Anticipada (porque es razonablemente previsible la imposibilidad de tal práctica en el momento ordinario) o de Prueba Preconstituida (porque por la fugacidad del objeto sobre el que recae, no ha de poder ser reproducida el día de la celebración del juicio oral).

Fuera de estos supuestos excepcionales, la prueba a practicar en el juicio se encuadra en el apartado del interrogatorio del acusado, la prueba testifical, la prueba pericial o la prueba documental. Y en materia de prueba electrónica, la inmensa mayoría de los supuestos se encontrarán incardinados en lo que es la prueba documental, donde, a tenor de la LECrim (art. 726), es el Tribunal el que examinará por sí mismo los documentos a que se refiere dicha prueba, pero en ningún momento se prohíbe que dicho examen venga auxiliado por el personal técnico oportuno que clarifique o ayude a comprender el significado de tales documentos, en este caso electrónicos, de conformidad con lo prevenido en el artículo 230-

1 LOPJ¹, por lo que en determinados supuestos, de carácter complejo, será prácticamente imprescindible el apoyo externo en cuanto a la comprensión de los datos o incluso la mera conexión o ejecución del programa que los contenga.

Un supuesto hasta ahora excepcional, pero ya incorporado definitivamente en nuestro ordenamiento a raíz de la entrada en vigor de la modificación de la LECrim por LO 13/2003, de 24 de octubre, es el del uso de la videoconferencia: El actual artículo 731 bis establece que el tribunal, de oficio o a instancia de parte, por razones de utilidad, seguridad o de orden público, así como en aquellos supuestos en que la comparecencia de quien haya de intervenir en cualquier tipo de procedimiento penal como imputado, testigo, perito, o en otra condición resulte gravosa o perjudicial, podrá acordar que su actuación se realice a través de videoconferencia u otro sistema similar que permita la comunicación bidireccional y simultánea de la imagen y el sonido, de acuerdo con lo dispuesto en el apartado 3 del artículo 229 de la Ley Orgánica del Poder Judicial. Nótese que el artículo habla de “imputado” y no de “acusado”, por lo que parece indicarse que la validez de este artículo se circunscribe a los actos procesales llevados a cabo durante la instrucción, pero no para aquellos relativos a la celebración de la vista oral, donde, de conformidad con el resto del articulado, sólo se permite la ausencia física del acusado en los supuestos excepcionales que, dentro del procedimiento abreviado, se recogen en el art. 786. De ahí que la Instrucción 1/2002 de la Fiscalía General del Estado ya estableciera que fuera de los supuestos establecidos legalmente (audición de testigos o peritos entre países miembros de la Unión Europea, posibilidad de utilización de cualquier medio técnico para evitar confrontaciones visuales a menores) el uso de la videoconferencia para la celebración del juicio oral en lo que se refiere a distanciamiento físico de acusado y Tribunal sólo podía ser considerado válido si así lo contemplara una norma legal explícita, por afectar significativamente a los principios de oralidad, inmediación y contradicción que deben regir en todo tipo de procesos penales. Y si bien esta doctrina se modificó de algún modo por la Instrucción 3/2002², dictada al mes siguiente, la conclusión final es la de valorar en cada caso concreto la oportunidad del uso de los medios electrónicos como sustitutivos de la presencia física como norma general, siguiendo siempre el criterio de proporcionalidad y motivación en la resolución que los adopte.

En principio, la mejor manera de obtener evidencias de la perpetración de un delito mediante un ordenador es tener acceso a dicho ordenador, no sólo para cerciorarnos de que el delito se ha cometido por medio de dicho terminal, sino también porque nos permitirá descubrir otro tipo de evidencias, alojadas en el propio ordenador o en sus cercanías (disquetes, CD-ROM...). Y ante la rapidez con que dichas evidencias pueden ser eliminadas por el usuario, es necesaria también una actuación policial rápida y precisa para evitar la destrucción de pruebas. Esta rapidez en la actuación policial no sólo es conveniente, sino incluso exigida en determinados temas, como ocurre con lo previsto en la Decisión del Consejo de Europa, de 29 de mayo de 2000, relativa a la lucha contra la pornografía infantil en Internet, donde, en su artículo 1-3, establece que "los Estados miembros garantizarán una actuación rápida de las autoridades policiales en cuanto reciban

¹ “Los Juzgados y Tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establece la Ley Orgánica 5/1992, de 29 de octubre, y demás Leyes que resulten de aplicación”

² Por la ratificación ocurrida en octubre de 2000 del Estatuto de la Corte Penal Internacional aprobado en Roma el 17 de julio de 1998, cuyo artículo 63-2 apunta que si el acusado perturbare continuamente el juicio, el Tribunal podrá disponer que salga de la Sala y «... observe el proceso y dé instrucciones a su defensor desde fuera, utilizando, en caso necesario, tecnologías de comunicación».

información sobre supuestos casos de producción, tratamiento, posesión y difusión de material pornográfico infantil. Las autoridades policiales podrán posponer su actuación si fuere necesario por razones tácticas y durante todo el tiempo requerido, a fin, por ejemplo, de llegar hasta los responsables de las operaciones delictivas o las redes (redes de pornografía infantil)".

El acceso desde un equipo informático a otro se hace siempre por medio de vía telefónica o de datos, lo que permite disponer de un instrumento de acceso (módem o router) que conecta a su vez la computadora con la Red, que por su parte está conectada (o puede estarlo) con los dispositivos de almacenamiento, por lo general *a mano* del usuario (Aunque no necesariamente... Piénsese en los complejos sistemas de almacenamiento alojados en la propia Red, como XDrive y similares...). De ahí que se trate de una cadena lógica: Identificado el emisor telefónico, se identifica la dirección electrónica del ordenador, que está alojado en un domicilio o local, donde también se hallan los sistemas de almacenamiento. Por ello es esencial la identificación del abonado conectado al servicio telefónico, como primer paso en el momento de concretar la imputación. Piénsese que, además, el artículo 400 del Código Penal castiga "la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador, aparatos, específicamente destinados a la comisión de delitos de falsificación", entre los cuales indudablemente entrarían los programas copiadores y utilidades de *hacking*.

La interesante Consulta 1/99 de la Fiscalía General del Estado abordó el problema de si es necesario o no un mandamiento judicial no para interceptar la comunicación en sí, sino incluso para que la compañía operadora facilite la identificación del abonado que haya hecho uso de la conexión en el lapso de tiempo especificado en la investigación. Ante la postura de entender que la necesidad de mandamiento judicial implicaría una restricción de las facultades de investigación del fiscal en la medida en que el artículo 5.2 del Estatuto Orgánico del Ministerio Fiscal reduce la legitimación para la adopción de medidas de investigación a aquéllas que no sean limitativas de derechos, por lo que la selección del régimen constitucional de garantía que le cuadra a este tipo de datos y contenidos no debe ser el estatuto de inviolabilidad del artículo 18.3 de la Constitución española (que sólo operaría cuando el acto de comunicación es interceptado en tiempo real, mientras se produce la transferencia del mensaje), sino la libertad informática del artículo 18.4 de la Constitución española (por considerar que el bien protegido es el libre flujo de las comunicaciones, de modo que, extinguida la comunicación, los datos que se registran en soporte informático para la facturación del servicio prestado quedarían sujetos al régimen específico de la LOPD 15/1999, de 13 de diciembre (e incluso antes, en la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal –LORTAD–), que no exige habilitación judicial para la cesión de información en favor del Ministerio Fiscal³, la Fiscalía General opta por considerar, de la misma forma que ya lo había hecho el Tribunal Europeo de Derechos Humanos (Sentencia de 2 de agosto de 1984 –caso *Malone*–⁴ o Sentencia de 30 de julio de 1998 –caso *Valenzuela Contreras*–⁵), que la

³ A favor de esta última tesis también se argumenta que la legislación de telecomunicaciones distingue conceptualmente entre interceptación de contenidos y acceso a los datos de tráfico, entre los que se incluyen los datos de identidad de los comunicantes, y que, de conformidad con el artículo 51 de la Ley 11/1998, de 24 de abril, general de telecomunicaciones, sólo la interceptación del contenido exige licencia judicial, lo que, *sensu contrario*, conduce a estimar no abarcados en el secreto de las comunicaciones los aspectos e informaciones no comprendidos en el contenido mismo, o el propio artículo 3.2 de la Ley 24/1998, de 19 de julio, del servicio postal universal, que, en relación con los datos sobre la existencia del envío, clase, identidad del remitente y destinatario, y sus direcciones, remite a la aplicación de la Ley orgánica 5/1992, de 29 de octubre.

⁴ "En relación con las comunicaciones telefónicas, el titular del servicio que registre mediante un contador los números que han sido marcados desde un determinado aparato obtiene una información de la que no puede hacerse uso sin la previa autorización del afectado."

inviolabilidad de las comunicaciones afecta no sólo al contenido del mensaje, sino incluso a constatar la existencia de la comunicación, duración de la misma y otras circunstancias que permitan ubicar temporal o espacialmente el proceso de la transmisión, si bien no sólo amparada en el secreto a las comunicaciones (dado que la comunicación o bien ya ha concluido o ni siquiera ha empezado), sino tangencialmente en el derecho a la protección de datos personales asociados a dichas comunicaciones⁶. Y continúa estableciéndose, en concordancia con la Circular 1/99, un triple *status* de las intervenciones electrónicas, atendiendo a la adopción de la medida de control (adoptada en el seno de un proceso penal, mediante auto judicial motivado, sobre la base de la apreciación de indicios delictivos⁷, delimitada subjetivamente⁸ y objetivamente, con duración limitada y proporcionalidad), en su ejecución (también controlada judicialmente) y en su incorporación al proceso (por medio de su transcripción e incorporación de las cintas originales a la causa).

El Convenio sobre Cibercriminalidad del Consejo de Europa (Budapest, 23/XI/2001) incide en este tema, ya que el artículo 18 establece que cada una de las partes adoptará las medidas legislativas pertinentes [...] para habilitar a sus autoridades competentes a ordenar a una persona presente en su territorio comunicar los datos informáticos específicos que estén bajo el control de esta persona además de almacenados en un sistema informático o en un soporte de almacenamiento informático, y, a un proveedor de servicios que actúe en el territorio de la Parte, comunicar los datos relativos al abonado⁹ que estén en su posesión o bajo su control [...], e incluso, ya en su artículo 16, obliga a adoptar las medidas legislativas pertinentes para permitir a las autoridades competentes ordenar u obtener de otro modo la rápida conservación de datos electrónicos, incluidos los datos relativos al tráfico cuando haya razones para pensar que éstos son particularmente sensibles a los riesgos de pérdida o modificación, incluidos los datos sujetos a custodia de corta duración¹⁰.

En Derecho comparado, existen múltiples propuestas que podrían refundirse en las posturas mantenidas por Estados Unidos, Alemania y Gran Bretaña, en orden de mayor a menor nivel de protección del derecho al secreto de las telecomunicaciones: Estados Unidos es, por tradición y experiencia en el uso (y abuso) de la red de redes, quien más se

⁵ "Se trata de una injerencia de la autoridad pública, en el ejercicio del derecho al respeto de la vida privada y de la correspondencia, el registro mediante un aparato contador de los números de teléfono marcados desde un determinado aparato, aun cuando este tipo de vigilancia no implique acceso al contenido de la conversación."

⁶ Sin embargo, esta línea no es unánime: en contra está la STS 459/99, de 22 de marzo, o la Sentencia del Juzgado de lo Penal n° 2 de Barcelona, de 28 de mayo de 1999 –caso *Hispaback*.

⁷ Los indicios racionales de criminalidad son datos externos que, apreciados judicialmente, conforme a las normas de recta razón, permiten descubrir o atisbar, sin la seguridad de la plenitud probatoria pero con la firmeza que proporciona una sospecha fundada, es decir, razonable, lógica, con arreglo a las reglas de la experiencia, la responsabilidad criminal de la persona en relación con el hecho posible objeto de investigación por medio de la interceptación telefónica –Auto del TS, de 18 de junio de 1992–, debiendo ofrecer la policía al juez la razón de ciencia, es decir, los motivos en que base su sospecha para que el juez esté en condiciones de apreciar si se trata realmente de una sospecha razonable y fundada y, si en consecuencia, la intervención que se solicita es proporcional al interés criminalístico invocado por los agentes de la autoridad –STS 1357/1998, de 10 de noviembre.

⁸ Ya sea el aparato intervenido propiedad del sujeto investigado o no, siempre y cuando éste lo utilice en sus comunicaciones (STS 606/1994, de 18 de marzo)

⁹ El Convenio de Budapest añade que los "datos relativos a los abonados" designa toda aquella información contenida bajo la forma de datos informáticos (...) que se refiera a sus usuarios, además de los datos relativos al tráfico o al contenido, y que permitan establecer (1) el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas a estos efectos y el periodo de servicio; (2) la identidad, la dirección postal o geográfica y el número de teléfono del usuario, además de cualquier otro número de acceso, datos relativos a la facturación y el pago, disponibles sobre la base de un contrato o arrendamiento de servicios; (3) cualquier otra información relativa al lugar donde se encuentren los equipos de comunicación, disponible sobre la base de un contrato o arrendamiento de servicio.

¹⁰ De ahí que, una vez que dicho Convenio sea ratificado por España y se convierta en texto legal vigente en nuestro país, como tratado internacional, se obligará al Estado español a introducir leyes de apoyo que regulen el acceso a los datos relativos a los usuarios, principalmente de identidad, cuenta corriente, dirección postal... para que se zanje de una vez la polémica de si es necesario o no mandamiento judicial para obtenerlos y en qué supuestos.

ha esforzado en delimitar el contenido y ámbito de las resoluciones judiciales tendentes a la intervención electrónica, con lo que se ha puesto de relieve la prohibición de autorizaciones judiciales de carácter genérico en cuanto a su objeto material (caso *Maryland contra Garrison*, 1987), aunque quepa cierta flexibilización en lo relativo al objeto a buscar, por imperativos tecnológicos (caso *US contra Reyes*, 1986), distinguiéndose la interceptación de comunicaciones *stricto sensu* de la interceptación de datos ya almacenados; ahora bien, a raíz del ataque terrorista del 11 de septiembre de 2001, tal postura se ha endurecido: La *USA Patriot Act of 2001*, de 26 de octubre de 2001, incluye como *ciberterrorismo* todos aquellos ataques vía Internet que causen pérdidas superiores a los 5.000\$, de modo que los *hackers* (intrusos) pueden sufrir condenas de hasta 20 años de cárcel y se obliga a las empresas de Internet a entregar el registro de actividad y los correos electrónicos de un sospechoso. Alemania establece un elenco de delitos graves para los que cabe la concesión de mandamientos judiciales de intervención (que podrán ser dictados incluso por el fiscal en caso de urgencia, con ratificación del juez en el plazo de tres días). El Reino Unido (*Interception of Communications Act*, 1985, y *Regulation of Investigation Power Act*, 2000) adopta una postura extremadamente poco garantista (con la atribución de inmensas facultades a la policía en orden a la intervención de comunicaciones, tanto en lo referente a contenidos como de datos de identificación).

Una vez obtenido el oportuno mandamiento judicial para averiguar la identificación del usuario (normalmente escindido en dos tipos de resoluciones judiciales distintas, la que intenta averiguar la dirección electrónica y el momento de conexión –dirigida al proveedor de acceso, como empresa que permite acceder a las redes de comunicación entre ordenadores, poniendo a su disposición una conexión TCP/IP– y la que intenta averiguar la identidad del abonado –dirigida al proveedor de servicios, como empresa titular de la infraestructura de comunicaciones–), cabe que o bien se tenga suficientes datos para proceder a una intervención policial inmediata, o bien sea necesaria una nueva resolución judicial, de interceptación de comunicaciones, que en la materia que nos ocupa suele apoyarse en la utilización de *sniffers* (rastreadores), mediante la grabación en el correspondiente soporte de las trasferencias telemáticas (normalmente mensajería electrónica), con una exacta reglamentación en la dirigida a la interceptación de comunicaciones orales (requisitos, plazo de interceptación y garantías, tal y como se consagran en la STC 49/99, de 5 de abril)¹¹, pero, en uno u otro caso, de tratarse de un terminal alojado en un domicilio particular, sería necesario un nuevo mandamiento judicial para proceder a la entrada en dicho domicilio, no tanto en lo que concierne al mismo ordenador¹², sino por cuanto el entorno físico del mismo comprende estancias en las que desarrolla la vida cotidiana del autor, como cualquier otro domicilio. Por ello, a pesar de la bienintencionada voluntad de las autoridades a la hora de llevar a cabo una rápida intervención policial, en determinados supuestos (como el intercambio mediante correo electrónico de ficheros conteniendo imágenes de pornografía infantil) es necesario hasta un número de cuatro resoluciones judiciales, todas ellas con sus oportunas motivaciones, para

¹¹ El Convenio del Consejo de Europa también recoge este supuesto, al establecer el artículo 21 que "[...] cada una de las partes adoptará medidas legislativas [...] para habilitar a sus autoridades competentes con relación a infracciones graves a definir por cada uno de los ordenamientos internos, a recopilar o grabar mediante la aplicación de los medios técnicos existentes en su territorio y obligar a un proveedor de servicios, dentro de sus capacidades técnicas existentes, a recopilar o grabar mediante la aplicación de los medios técnicos existentes en su territorio o prestar asistencia a las autoridades competentes y cooperar con ellas para la recopilación o grabación, en tiempo real, de datos relativos al contenido y en relación con comunicaciones precisas en su territorio transmitidas mediante un sistema informático [...]"

¹² Aunque no es descabellado, como opina Álvarez Cienfuegos, que se realizara una abstracción del concepto de domicilio como tal, para extenderlo al mismo ordenador, a guisa de domicilio virtual.

llegar a acceder físicamente a una máquina y su contenido, sin que se tenga siquiera entonces la certeza de haber conseguido un cúmulo tal de pruebas suficiente para imputar el delito a su autor¹³. De ahí los esfuerzos, incluso a escala internacional, de unificar actuaciones y de lograr la concienciación de la globalidad de los servidores y usuarios de Internet en orden a la represión de tales delitos¹⁴.

En lo que se refiere a la intervención en sí del contenido de la comunicación, la norma básica en nuestro ordenamiento sigue siendo el artículo 579 de la Ley de enjuiciamiento criminal, que obliga a que el mandamiento judicial se acuerde en el seno de una causa criminal abierta, tanto en su modalidad de detención de la comunicación como en su mera observación, por lo que tal medida debe ser (por su excepcionalidad en cuanto cortapisa del secreto de las comunicaciones) idónea y proporcional a la búsqueda realizada. Si se trata de mensajes de correo electrónico, dada su especial naturaleza (se remiten por vía telefónica o de datos –lo cual lo asimila a una comunicación telefónica–, pero se almacenan en un buzón electrónico hasta que es descargado por el usuario, que puede (o no) conservarlo en un dispositivo de almacenamiento –lo cual lo asimila a una carta postal–), resulta más lógica¹⁵ la aplicación del régimen de intervención de despachos telegráficos de los artículos 582 y 583 de la Ley rituarial que el de las comunicaciones telefónicas del artículo 579, dado el mayor grado de control judicial y técnico de las mismas, aunque en un caso u otro, con el sigilo (secreto¹⁶ y confidencialidad¹⁷) que la materia entraña.

Una vez que el material informático está en manos de los miembros de la policía, debe garantizarse, como ocurre en cualquier tipo de entrada y registro, que el material incautado pueda ser examinado por el personal técnico oportuno en su identidad e integridad, esto es, preservando la posibilidad de que pueda existir la mínima duda acerca de que lo examinado no sea *exactamente* lo ocupado en la actuación, mediante el bloqueo y precintado de cualquier ranura (*slot*), puerto o disquete hasta el momento mismo del examen pericial o de la extracción de información que permita efectuarlo, por medio del volcado de datos en el soporte lógico adecuado, todo ello reservando las garantías que, en orden a la fe pública judicial, se establecen, como si de una apertura de paquete, postal o no, se tratase en nuestro ordenamiento. Y así, dada la especial naturaleza de los documentos digitales, puede efectuarse una copia exacta e íntegra del contenido de un disco duro, un CD-ROM, etc.,

¹³ Lo cual es bastante frecuente para supuestos en que el mensaje se halle cifrado: En algunos países, por tal motivo, se ha prohibido o limitado el uso de la criptografía.

¹⁴ La Decisión del Consejo de Europa de 29 de mayo de 2000, en su artículo 1, establece que "los Estados miembros adoptarán las medidas necesarias para animar a los usuarios de Internet a que comuniquen a las autoridades policiales, directa o indirectamente, sus sospechas sobre la difusión de material pornográfico infantil en Internet, cuando encuentren material de este tipo. Se dará a conocer a los usuarios de Internet los modos de ponerse en contacto con las autoridades policiales o con las entidades que tengan vínculos privilegiados con éstas, a fin de que dichas autoridades puedan cumplir su cometido de prevención y lucha contra la pornografía infantil en Internet"; en su artículo 3, por otra parte, establece que "los Estados miembros intercambiarán experiencias sobre la eficacia de las medidas que hayan adoptado para eliminar la pornografía infantil en Internet. En este contexto, examinarán las medidas siguientes, que serían obligatorias para los proveedores de Internet: a) informar a las entidades competentes acerca del material de pornografía infantil del que hayan recibido información o tengan conocimiento y que se difunda a través de ellos; b) retirar de la circulación el material de pornografía infantil del que tengan conocimiento y que se difunda a través de ellos, salvo que las autoridades competentes dispongan otra cosa; c) conservar, de conformidad con lo enunciado en la Resolución del Consejo, de 17 de enero de 1995, sobre la interceptación legal de las telecomunicaciones, datos de tráfico, cuando haya lugar y sea técnicamente viable, en particular a efectos de la persecución penal en caso de sospecha de abuso sexual de menores, así como de producción, tratamiento y difusión de pornografía infantil, durante todo el tiempo especificado en la ley nacional aplicable, a fin de que estos datos estén disponibles para su inspección por parte de las autoridades policiales de conformidad con las normas de procedimiento aplicables; d) crear sistemas propios de control destinados a combatir la producción, el tratamiento, la posesión y la difusión de material pornográfico infantil".

¹⁵ En este sentido, Hernández Guerrero y Álvarez de los Ríos. (1999). "Medios informáticos y proceso penal". Estudios Jurídicos del Ministerio Fiscal, IV.

¹⁶ Así, la Circular 1/99 de la Fiscalía General del Estado.

¹⁷ Así, el Convenio del Consejo de Europa, en diversos puntos de su articulado (20-3, 21-3...).

siempre en presencia del secretario judicial, como titular de la fe pública judicial, para trabajar sobre ella. Debe tenerse en cuenta que cualquier manipulación, por pequeña que sea, altera el contenido de un ordenador, ya sea en los ficheros de registro del sistema operativo o de otro tipo, sin olvidar la posibilidad de que el usuario haya colocado las *trampas* que haya creído oportunas para destruir determinada información en caso de acceso no autorizado.

No obstante, el avance de las nuevas tecnologías, así como el de las medidas de seguridad adoptadas por los delincuentes a fin de evitar ser descubiertos, o al menos imputados, obliga a reflexionar sobre varios asuntos: Para el caso de que, al realizar el volcado de un sistema de almacenamiento nos hallemos ante un sistema protegido por medio de clave o encriptación que impida el adecuado estudio del contenido de los datos investigados, ¿cabe que pueda, incluso por medio de orden judicial, obligarse al sujeto a proporcionar la clave de acceso o el método de desencriptación?¹⁸ Pienso que no, ya que, a diferencia de lo que ocurría con proveedores de acceso o de servicios, cuya negativa a proporcionar los datos solicitados por la autoridad judicial puede ser constitutiva de un delito de obstrucción a la justicia o de desobediencia grave, en el presente supuesto nos hallamos ante un imputado, al que le ampara el derecho de no declarar contra sí mismo y que en modo alguno tiene obligación de facilitar la investigación dirigida contra él, a pesar de que dicha negativa pueda ser valorada por la autoridad judicial de la forma que crea oportuna, del mismo modo que puede ser valorada la negativa a contestar a los interrogatorios en la vista oral, pero sin que tal valoración pueda fundamentar de por sí un fallo condenatorio¹⁹. No obstante, se pueden utilizar programas específicos para conseguir la contraseña o clave sin que dicha operación suponga manipulación o alteración alguna del contenido del soporte, de la misma forma que en una diligencia de entrada y registro, no se puede obligar al titular de la residencia a que abra la puerta, pero nada impide que ésta sea tirada abajo por los miembros de las Fuerzas y Cuerpos de Seguridad en caso de riesgo plausible de destrucción de pruebas.

¹⁸ Sin embargo, y para el caso de emisiones en la Red de ficheros de cualquier tipo protegidos por procedimientos de cifrado, la Ley general de telecomunicaciones, de 24 de abril de 1998, en su artículo 52, prevé la posibilidad de imponer gubernamentalmente una política de depósito de claves, al poderse imponer a los fabricantes de hardware o software, a los operadores que incluyan cifrado en las redes e incluso a los usuarios la obligación de notificar los algoritmos de cifrado para su control.

¹⁹ Por sí misma, pero puede coadyuvar a que, de existir otros indicios de suficiente importancia, la balanza se decante en su contra. Como opina Hernández Guerrero, lo contrario podría fundamentar una atenuación de la pena, en relación con la persecución de delitos de tráfico de drogas o relacionados con la actuación de bandas armadas, al amparo de los artículos 376 y 579 del Código penal.