LA LEY
grupo Wolters Kluwer

La prueba electrónica en el proceso penal

Joaquín DELGADO MARTÍN

Magistrado de la Audiencia Provincial de Madrid. Doctor en Derecho

Diario La Ley, Nº 8167, Sección Doctrina, 10 Oct. 2013, Año XXXIV, Editorial **LA LEY**

LA LEY *7336/2013*

El presente trabajo se centra en la problemática relativa al acceso y análisis de la información contenida en dispositivos electrónicos, incluyendo tanto sistemas informáticos y cualesquiera aparatos informáticos o de tecnología digital, como los medios de almacenamiento masivo de memoria. De esta manera, no se analizarán los problemas que surgen en la investigación del delito ligados a la transmisión de los datos.

I. *CONCEPTO DE PRUEBA ELECTRÓNICA. MODALIDADES BÁSICAS*

Por prueba electrónica cabe entender **toda información de valor probatorio contenida en un medio electrónico o transmitida por dicho medio** (1) . En esta definición cabe destacar los siguientes elementos: se refiere a cualquier clase de información (2) ; que ha ser producida, almacenada o transmitida por medios electrónicos (3) ; y que pueda tener efectos para acreditar hechos (4) en el proceso abierto para la investigación de todo tipo de infracciones penales (5) , y no solamente para los denominados delitos informáticos (6) . De esta manera, la fuente de la prueba radica en la información contenida o transmitida por medios electrónicos, mientras que el medio de prueba será la forma a través de la cual esa información entra en el proceso (7) : normalmente como prueba documental o como prueba pericial, pero también incluso a través de la prueba testifical mediante el testimonio de la persona que ha tenido contacto con el dispositivo electrónico.

El elemento esencial que permite la construcción conceptual de este tipo de prueba radica precisamente en su naturaleza «electrónica» (8) , es decir, se utiliza un «lenguaje binario a través de un sistema que trasforma impulsos o estímulos eléctricos o fotosensibles y, por cuya descomposición y recomposición informática grabada en un formato electrónico, genera y almacena la información. Dicho lenguaje es un código ininteligible para aquéllos que no son informáticos. La visualización del texto en pantalla es una traducción en lenguaje alfabético común, descodificado» [GARCÍA TORRES (9)]. Y añade este autor que «entonces, entre lo conservado y lo exteriorizado no existe identidad. El archivo se conserva en un sistema binario. En cambio, el texto exteriorizado es fruto de la transformación de ese sistema binario en forma de escritura, ahora sí, con letras de nuestro alfabeto» (10) .

Dentro de este concepto de prueba electrónica, cabe distinguir dos modalidades básicas: en primer lugar, los datos o informaciones *almacenados* en un dispositivo electrónico; y, por otra parte, los que son *transmitidos* por cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras.

El presente trabajo se centra en la problemática relativa al **acceso y análisis de la**

información contenida en dispositivos electrónicos, incluyendo tanto sistemas informáticos y cualesquiera aparatos informáticos o de tecnología digital, como los medios de almacenamiento masivo de memoria (11) . De esta manera, no se analizarán los problemas que surgen en la investigación del delito ligados a la transmisión de los datos.

II. *NORMATIVA REGULADORA DE LA PRUEBA ELECTRÓNICA*

En la actualidad no existe una regulación específica de esta materia en la Ley de Enjuiciamiento Criminal, sino que frecuentemente han de aplicarse las normas que la misma contiene para materias análogas, teniendo siempre como referencia la doctrina que la jurisprudencia viene construyendo sobre la injerencia en los derechos fundamentales en la investigación de los delitos. Ello genera determinadas incertidumbres en la actuación del sistema penal, que están afectando a su propia eficacia.

Por ello resulta imprescindible que la **nueva Ley de Enjuiciamiento Criminal** proceda a regular expresamente el acceso a la información contenida en dispositivos electrónicos y su incorporación al proceso penal, eliminando incertidumbres con pleno respeto a las garantías del proceso, especialmente cuando puedan verse afectados derechos fundamentales de las personas. De esta manera, España cumplirá con las obligaciones derivadas de la ratificación del Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2011, que resulta aplicable no solamente a los denominados delitos informáticos, sino también «a la obtención de pruebas electrónicas de cualquier delito» [art. 14.2 c) del Convenio]. Cabe valorar positivamente que la propuesta de Texto articulado de Ley de Enjuiciamiento Criminal (2013) (12) , en adelante PLECrim.-2013, contenga un Capítulo en el que regula el «Registro de dispositivos de almacenamiento masivo de información» (arts. 347 y ss.) y otro Capítulo relativo a los «Registros remotos sobre equipos informáticos» (arts. 350 y ss.).

Por otra parte, la regulación legal ha de ser completada con una **normativa reglamentaria y/o una protocolización/homologación de actuaciones**. La Ley no puede regular cada uno de los aspectos de esta materia, especialmente compleja en muchas ocasiones, sino que ha de existir una normativa complementaria que regule aspectos tales como las formas de acceso a las pruebas electrónicas, las singularidades de la cadena de custodia con la finalidad de garantizar su autenticidad e integridad, diferentes cuestiones sobre la realización de la prueba pericial informática, entre otras.

Esta necesidad deviene aún más relevante si se tienen en cuenta los rápidos avances en las tecnologías de la información y de la comunicación, que generan nuevas necesidades (realidad criminológica) y elementos (modernas técnicas para acreditar los elementos de la infracción penal) en la investigación de los delitos. La normativa complementaria permitirá que la actuación del sistema penal pueda ir adaptándose a las nuevas realidades, compatibilizando la flexibilidad con las necesidades de la seguridad jurídica, teniendo en cuenta las recomendaciones y otros documentos elaborados por entidades con reconocimiento científico, como por ejemplo la *ENFSI-European Network of Forensic Science Institutes* (13) .

En todo caso, este trabajo pretende profundizar en el tratamiento de la prueba electrónica en el proceso penal atendiendo al Derecho vigente en este momento.

III. *ACCESO A LAS PRUEBAS ELECTRÓNICAS DURANTE LA INVESTIGACIÓN DEL DELITO*

1. *Formas de acceso*

La propia multiplicidad de los instrumentos y elementos tecnológicos determina una heterogeneidad de las formas de acceder a su contenido, pudiendo distinguirse varias modalidades básicas. La primera consiste en el acceso al contenido del sistema o equipo mediante su posesión material o física, tras haber sido aprehendido por la autoridad competente. Y dentro de esta categoría podemos distinguir dos supuestos diferentes: aprehensión del propio dispositivo electrónico encontrado fuera de lugar cerrado; y diligencia de entrada y registro en lugar cerrado con ocupación del dispositivo o de la información relevante.

En segundo lugar, también existe la posibilidad técnica de acceder al contenido de un sistema informático sin necesidad de proceder a la aprehensión física del equipo informático, a través de lo que pueden denominarse registros remotos (*remote search*). Asimismo es posible el acceso a información contenida en un servidor o sistema pero accesible desde otro al que se haya accedido de forma tradicional o por registro remoto. La cuarta modalidad radica en la aportación al proceso de la prueba electrónica por alguna de las partes. Por último, hay que analizar las especificidades propias del llamado registro transfronterizo, es decir, cuando los datos se encuentran almacenados en un sistema informático o servidor situado fuera del territorio nacional.

2. *Derechos fundamentales afectados*

«La versatilidad tecnológica que han alcanzado los teléfonos móviles convierte a estos terminales en herramientas indispensables en la vida cotidiana con múltiples funciones, tanto de recopilación y almacenamiento de datos como de comunicación con terceros (llamadas de voz, grabación de voz, mensajes de texto, acceso a internet y comunicación con terceros a través de internet, archivos con fotos, videos, etc.) (14) ». Por ello, el acceso a la información contenida en los dispositivos electrónicos puede afectar a varios derechos fundamentales:

- **Afecta en todo caso a la intimidad personal** (art. 18.1 CE), por lo que únicamente será legítima la injerencia si concurre la autorización judicial previa o bien el consentimiento del afectado (STC 173/11 de 7 de noviembre, FJ 5.º), sin perjuicio de la intervención policial en casos de urgente necesidad con pleno respeto al principio de proporcionalidad (STC 115/2013).
- También puede existir una injerencia en el **secreto a las comunicaciones** (art. 18.3 CE), en aquellos casos en los que pudiera desvelar procesos comunicativos (STC 115/2013, FJ 4.º), es decir, el acceso a datos que formen parte de un proceso de comunicación (15) vigente. Si la información se refiere a una comunicación ya terminada o consumada, en principio solamente se vería afectado el derecho a la intimidad, aunque una interpretación favorable a la garantía del secreto de las comunicaciones puede conducir a entender afectado este derecho en determinados supuestos (16) .
- Asimismo puede verse afectado el derecho a la inviolabilidad domiciliaria (art. 18.2 CE) cuando el dispositivo electrónico se encuentre en el interior de un lugar cerrado constitutivo de domicilio.
- Incluso puede desplegar efectos sobre el derecho a la autodeterminación informativa en el ámbito de la protección de datos personales (17) (art. 18.4 CE).

IV. *APREHENSIÓN DE DISPOSITIVO FUERA DE LUGAR CERRADO*

Esta primera modalidad hace referencia a aquellos casos en los que se procede a la incautación

o aprehensión de un dispositivo electrónico que se encuentra fuera de un lugar cerrado, bien en poder de una persona o bien abandonado en una determinada zona.

En algunos ámbitos doctrinales (18) se viene señalando la dificultad de la práctica de estos registros al margen de una diligencia de entrada y registro en lugar cerrado, porque no existe en la actualidad una regulación legal expresa de este supuesto. Sin embargo, han sido admitidos por la jurisprudencia con la exigencia de los presupuestos para la injerencia en el derecho a la intimidad, con la aplicación analógica de las normas del registro en lugar cerrado contenidas en la Ley de Enjuiciamiento Criminal.

Cabe distinguir varios momentos distintos: la aprehensión o incautación del dispositivo; el registro de su contenido, es decir, el acceso a la información contenida en su interior; y la obtención o confiscación de los datos.

1. *Régimen de la aprehensión o incautación del dispositivo*

La Policía Judicial (art. 282 LECrim.) o el propio Juez de Instrucción (art. 326.1.º LECrim.) pueden recoger aquellos dispositivos electrónicos que han de ser utilizados como medio de prueba en un proceso penal (19) por contener información relevante para la acreditación de los elementos y circunstancias del delito. Estos dispositivos se han de incorporar al proceso bajo la responsabilidad del Secretario Judicial, o quedarán conservadas a disposición judicial en organismo adecuado para su depósito (art. 338 LECrim.) (20) .

Recordemos que los dispositivos electrónicos pueden ser ocupados o aprehendidos en tres supuestos (21) : como cuerpo del delito, es decir, la cosa objeto de la infracción penal o contra la que se ha dirigido el hecho punible; como instrumentos del delito, esto es, los medios u objetos a través de los cuales se ha llevado a cabo la comisión de la infracción penal; y como piezas de convicción, entendidas como los objetos, huellas y vestigios que, no estando incluidas en las dos categorías anteriores, tienen relación con el delito y pueden servir de prueba o indicio en la comprobación de la existencia, autoría o circunstancias del hecho punible.

2. *Registro del dispositivo*

Una vez ocupado el dispositivo electrónico, el acceso a los datos o información que se encuentran en su interior afecta en todo caso al derecho fundamental a la intimidad, que ha de someterse necesariamente al régimen de la previa autorización judicial o consentimiento del afectado, sin perjuicio de la actuación de la Policía Judicial en los supuestos de urgencia.

3. *La obtención o confiscación de los datos*

Tras el registro del dispositivo electrónico, resulta necesario incorporar al proceso aquellos datos que sean relevantes para la prueba de los elementos del delito investigado.

En primer lugar, la información puede ser presentada ante el órgano judicial mediante la aportación del propio sistema o equipo de almacenamiento, que será reproducido y examinado por el tribunal (como prueba documental de conformidad con el art. 726 LECrim.) con los medios técnicos que resulten necesarios, y que frecuentemente estarán a disposición del órgano judicial: por ejemplo, ordenador para la lectura de dispositivos USB o de DVD, dotado del programa informático adecuado para el concreto formato de archivo de que se trate. En

segundo lugar, también puede realizarse mediante la incorporación al proceso de una copia de la información del mismo que sea relevante para el proceso (volcado); únicamente han de ser ocupados aquellos dispositivos que resulten estrictamente necesarios para la tramitación del proceso (argumento *ex* art. 574 LECrim.), procediendo en otro caso únicamente a la ocupación de los datos.

Asimismo *en ocasiones será necesaria la realización de un análisis de la información del sistema o equipo que solamente puede ser afrontada con conocimientos especializados en la materia, a través de la práctica de un dictamen de peritos o prueba pericial informática* que actuará sobre una copia o clonado de los datos.

V. *REGISTRO DEL SISTEMA INFORMÁTICO QUE SE ENCUENTRA EN LUGAR CERRADO*

1. *Régimen de la entrada y registro en lugar cerrado*

Resulta frecuente que los dispositivos electrónicos se encuentren en un lugar cerrado, por lo que el acceso y examen de su contenido se realiza en el seno de una diligencia de entrada y registro, con aplicación de su régimen jurídico [arts. 573 y ss. LECrim. (22)].

En primer lugar, la entrada y registro puede llevarse a cabo en un *lugar cerrado no constitutivo de domicilio,* es decir, cualquier lugar aislado o acotado respecto del exterior (23) que no pueda ser considerado domicilio (24) . La diligencia debe ser realizada con pleno sometimiento a los requisitos de legalidad ordinaria contenidos en los arts. 546 y ss. LECrim., entre las que cabe destacar la autorización judicial (art. 546) y la presencia del interesado (art. 569). Cuando ha sido previamente autorizada por el Juez y realizada con todos los requisitos exigidos por la Ley de Enjuiciamiento Criminal, especialmente la presencia en el acto del Secretario Judicial, adquiere el valor de prueba preconstituida y puede enervar la presunción de inocencia siempre que sea leída en el acto del juicio conforme a lo dispuesto en el art. 730 LECrim. (25) . En la doctrina se discute la posibilidad de que sea realizada por la Policía sin necesidad de autorización judicial previa (26) : una postura defiende esta autorización en todo caso, otra entiende que solamente es necesaria cuando ya existe una causa judicial abierta, mientras que una tercera no la considera precisa (27) ; en todo caso, en este supuesto no se vulneran los derechos fundamentales a la inviolabilidad del domicilio y a la intimidad (28) , por lo que su resultado podrá ser valorado como prueba de cargo siempre que acceda al juicio a través de una de las pruebas aptas para enervar la presunción de inocencia, señaladamente la declaración en el plenario como testigos de los policías intervinientes (29) .

En segundo término, la diligencia de entrada y registro puede ser realizada en el *domicilio* de una persona física o jurídica. Cuando se realiza sin autorización judicial previa (30) , o sin que dicha resolución cumpla todos los requisitos de motivación y proporcionalidad, se produce una vulneración del derecho fundamental a la inviolabilidad del domicilio (art. 18.2 Constitución) y, por tanto, deviene prueba nula por aplicación del art. 11.1 LOPJ, carente de toda eficacia probatoria; en este caso (31) , la sentencia no podrá fundamentarse (32) en los datos obrantes en los dispositivos electrónicos hallados; ni en los resultados de las pruebas que se proyecten sobre los citados dispositivos: dictámenes periciales (informáticos o similares), o las declaraciones testificales que tengan por objeto el reconocimiento de los mencionados objetos.

2. *Registro del dispositivo*

La autorización judicial de entrada y registro de un determinado lugar cerrado permite a los agentes intervinientes el registro de todas las dependencias y pertenencias que allí se encuentren, entre las que cabe incluir los dispositivos electrónicos que contengan o puedan contener evidencias de la comisión del delito investigado; todo ello sin perjuicio de que durante la diligencia se encuentren los denominados «hallazgos casuales», es decir, objetos o instrumentos de otras infracciones penales que no son objeto del proceso, lo que requerirá una nueva autorización judicial específica (33) .

En este sentido, la Sentencia del Tribunal Supremo 785/2008, de 25 de noviembre, al referirse a un supuesto en el que las pruebas de la comisión del delito de posesión y difusión de pornografía infantil (conversaciones de chat ya celebradas) se encontraban almacenadas en los equipos informáticos intervenidos en la diligencia de entrada y registro, afirma expresamente que «la Audiencia Provincial entiende y lo hace con acierto que el auto de entrada y registro comprende esta diligencia, por cuanto a la vista de la naturaleza del delito que se investigaba la policía estaba autorizada a recoger los objetos o instrumentos de los que pudiera deducirse la comisión del delito y que fueran hallados en el recinto registrado, y en este sentido se intervienen los ordenadores y su disco duro». Y añade posteriormente que «así pues, aunque había bastado el auto inicial, en el que no existe ninguna cortapisa en cuanto se trate de intervenir objetos o instrumentos o en general piezas de convicción que acrediten la comisión del delito investigado, la policía hizo una razonable y prudente interpretación del auto, sin excederse lo más mínimo de lo que constituía el propósito de la diligencia ordenada».

En todo caso, si consta que las pruebas del delito pueden encontrarse en dispositivos electrónicos localizados en un local cerrado (34) , resulta más adecuado que el auto de entrada y registro también autorice expresamente el registro de dichos dispositivos (35) .

3. *La obtención o confiscación de los datos*

Con carácter general, durante la práctica del registro pueden ocuparse aquellos elementos o equipos informáticos que sean necesarios para la investigación o para garantizar la pena de comiso o las responsabilidades pecuniarias que puedan derivarse del delito. De esta manera, puede ser objeto de aprehensión bien el propio dispositivo electrónico (y los instrumentos accesorios como pantallas, teclados, ratones, cables y otros similares), o bien únicamente datos o informaciones relevantes para el proceso.

Esta obtención de los datos se realiza de la misma forma analizada en el supuesto de registro fuera de lugar cerrado.

VI. *REGISTRO DE INFORMACIÓN ACCESIBLE*

1. *Concepto*

Desde el punto de vista del «continente» de la información, pueden distinguirse dos modalidades: en primer lugar, el acceso a los datos contenidos en el propio sistema informático o equipo de almacenamiento (registro tradicional); y en segundo término, el acceso a los existentes en otro sistema de información accesible desde el primero o disponible para éste (registro remoto).

Nos estamos refiriendo al creciente fenómeno de la deslocalización de la información, como

ocurre con las denominadas técnicas de computación en la nube o *cloud computing* en donde la información se almacena de manera permanente en servidores alojados en cualquier parte del mundo y se envía a través de Internet a cachés temporales del equipo informático del usuario (equipo portátil, equipo de sobresemesa, tableta, Smartphone…) (36) .

A) *Régimen jurídico*

Cuando, en el seno de una entrada en lugar cerrado autorizada judicialmente, se ha iniciado el registro de un concreto dispositivo electrónico y los investigadores conocen que una parte de la información se encuentra en otro sistema informático accesible o disponible desde el primero, solamente una rechazable interpretación extensiva de la autorización permitiría que los mismos accedieran a dicha información «en remoto» (37) . Por ello, y de forma análoga a los hallazgos casuales, los agentes intervinientes deberán solicitar autorización judicial para ampliar el registro al otro sistema accesible desde el primero, adoptando las cautelas necesarias mientras se tramita la misma. En sentido, el art. 19.2 del Convenio de Budapest se refiere a que el ordenamiento ha de contemplar la posibilidad de que las autoridades competentes procedan a ampliar rápidamente el registro o forma de acceso similar al otro sistema (38) .

Si se procede a la incautación policial de un dispositivo electrónico fuera de lugar cerrado, es necesario en todo caso que los agentes soliciten autorización judicial para registrar el contenido de los datos alojados en otro sistema accesible desde el primero; salvo que concurran razones de urgencia que justifiquen la necesidad de la intervención por parte de la Policía, tal y como ha admitido el Tribunal Constitucional en casos de injerencia en el derecho a la intimidad.

VII. *REGISTRO REMOTO: TROYANOS*

1. *Concepto y utilidad para la investigación*

Abordamos ahora aquel supuesto en el que se accede al contenido de un sistema informático sin necesidad de proceder a la aprehensión física del dispositivo electrónico, a través de lo que pueden denominarse registros remotos (*remote search*) o registros *on line*. Como afirma ORTIZ PRADILLO (39) , se trata de la técnica consistente en el acceso mediante la previa instalación en el sistema investigado de un software [los denominados «programas troyanos (40) »] que permita a las autoridades escanear un disco duro y demás unidades de almacenamiento y remitir de forma remota y automatizada el contenido del mismo al informático de la autoridad responsable de la investigación.

Este tipo de registros puede resultar útil en diferentes supuestos: cuando el dispositivo electrónico investigado se encuentra en constante movimiento, como en el caso de los smartphones, tabletas o similares; o en caso de que el intento de acceso al lugar donde se halle suponga un peligro para la vida o integridad física de los agentes, o bien un riesgo para la propia integridad de la información o del propio equipo informático, como puede ocurrir si el equipo cuenta con un programa de borrado o autodestrucción automática o si el imputado decide inmolarse con destrucción de los equipos (41) ; o cuando sea necesario acceder al equipo informático en vivo para capturar las claves utilizadas para descifrar el uso de criptografía en la información almacenada (42) ; entre otras posibilidades.

VELASCO NÚÑEZ (43) destaca diferentes ventajas de la utilización de los «troyanos»: exige menos efectivos investigadores que cualquier otra técnica tecnovigilante y capta muchísima más

información; se instala con alta movilidad, ya que opera a través de Internet mediante distintas máquinas, técnicas, plataformas y arquitecturas, de modo que es tan ubicua e instantánea como la actividad transnacional y transfronteriza que desarrolle el investigado; y aprovecha la tecnología para multiplicar la velocidad de conocimiento de la actividad investigada porque, según la concreta programación del software espía, éste busca y selecciona lo investigado más rápidamente que el propio agente facultado. Y como desventajas, el mismo autor señala que puede ser detectado por los programas antivirus, a no ser que se solicitase la impensable colaboración de los proveedores de antivirus; y para su instalación precisa de una conexión a Internet lo suficientemente seguida como para que dé tiempo a alojar el software.

2. *Régimen jurídico*

Los registros remotos, aplicables tanto a equipos informáticos como a teléfonos y otros dispositivos móviles (44), aportan un importante medio de investigación criminal y una relevante fuente de prueba del delito, especialmente en los supuestos en los que es necesaria una actuación ágil y rápida. En definitiva, un sistema penal no puede renunciar a la eficacia investigadora derivada de este tipo de registros.

Sin embargo, también suponen una injerencia de gran intensidad en los derechos a la intimidad y al secreto de las comunicaciones de la persona investigada, aunque también en el denominado derecho a la autodeterminación informativa del art. 18.4 Constitución, por lo que sería necesario contar con una legislación que regulara con suficiente calidad normativa sus presupuestos de ejercicio y su control judicial. Conviene destacar que el PLECrim.-2013 contiene un Capítulo que regula los «Registros remotos sobre equipos informáticos» (arts. 350 y ss.), exigiendo la previa autorización judicial para «la utilización de datos de investigación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que la medida resulte proporcionada para la investigación de un delito de especial gravedad y sea además idónea y necesaria para el esclarecimiento del hecho investigado, la averiguación de su autor o la localización de su paradero»; concretando posteriormente los requisitos de la autorización judicial.

Si se afirma la admisibilidad de los registros remotos en el marco del Derecho Procesal español vigente (45) , siempre ha de realizarse con pleno sometimiento a los criterios que la jurisprudencia ha construido desarrollando los derechos fundamentales recogidos en la Constitución en relación con otras injerencias, también en el ámbito de los sistemas de información y de las telecomunicaciones; y exigiendo a las autoridades y agentes del sistema penal un especial rigor tanto en la concurrencia de los presupuestos habilitantes ligados al principio de proporcionalidad, como en el control jurisdiccional de su ejecución. En este sentido, en el FJ 4.º de la STC 173/2011, de 7 de noviembre, se afirma que «cualquier injerencia en el contenido de un ordenador personal —*ya sea por vía de acceso remoto a través de medios técnicos* (46) , ya como en el presente caso, por vía manual— deberá venir legitimada en principio por el consentimiento de su titular, o bien por la concurrencia de los presupuestos habilitantes antes citados».

VIII. *REGISTROS TRANSFRONTERIZOS*

En los casos de registro de información accesible, así como en los registros remotos, surge un problema añadido cuando los datos se encuentran almacenados en un sistema informático o servidor situado fuera del territorio nacional, encontrándonos ante el llamado «registro transfronterizo» (47) . El Convenio de Budapest se refiere a estos registros distinguiendo varias posibilidades que se examinan a continuación.

1. *Fuente abierta. Consentimiento*

La Autoridad investigadora podrá acceder a los datos que se encuentren almacenados fuera del territorio de su jurisdicción en dos supuestos (art. 32 del Convenio): por un lado, cuando se trate de datos informáticos almacenados que se encuentren a disposición del público (fuente abierta); y por otro lado, cuando conste el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos por medio de ese sistema informático.

2. *Cooperación judicial internacional*

Fuera de los casos del apartado anterior, la Autoridad investigadora deberá remitir la correspondiente solicitud de asistencia judicial internacional con fundamento en el propio Convenio de Budapest, o bien en otro tratado o instrumento internacional que resulte de aplicación. En este sentido, el art. 31 del Convenio de Budapest regula un supuesto de asistencia mutua en el que un Estado puede solicitar a otro que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida.

En el seno de la UE puede contribuir a la agilidad de la asistencia judicial la aplicación de la orden europea de embargo o aseguramiento de prueba regulada por Decisión Marco de 22 de julio de 2003 y desarrollada en España por la Ley 18/2006, que puede ser utilizada para todo tipo de pruebas electrónicas, tanto para datos como para los propios dispositivos electrónicos (48) . A través de esta orden puede solicitarse la retención de los datos afectados; y posteriormente la autoridad de emisión deberá pedir la entrega o transmisión de dichos datos al amparo del instrumento internacional que cubra dicha actuación, pudiéndose utilizar para ello el Convenio de Budapest sobre Ciberdelincuencia u otro convenio aplicable (49) .

IX. *APORTACIÓN DE LA PRUEBA ELECTRÓNICA POR LAS PARTES*

Durante la fase de instrucción cualquiera de las partes puede, en primer lugar, aportar una prueba electrónica al proceso solicitando la unión a los autos del propio dispositivo en el que se encuentre la misma, pudiendo también acompañar una copia en papel con la transcripción de la información relevante (50) . En segundo lugar, puede solicitar al Juez que reclame la remisión de una prueba o documento electrónico, designando oportunamente el lugar o archivo en el que se encuentre. Asimismo se podrá practicar algún dictamen pericial sobre la mencionada prueba electrónica, ya sea a instancia de parte o porque el Juez considere necesario realizarla de oficio o a la vista de las alegaciones de impugnación de la otra parte.

Posteriormente, la parte interesada podrá introducir la prueba electrónica en el juicio oral proponiéndola como prueba documental que, una vez admitida, será objeto de examen por el tribunal al amparo del art. 726 LECrim.; insertándose en el debate procesal con sometimiento a la contradicción de las partes, quienes podrán impugnar su contenido, su forma de acceso al proceso y sus condiciones de autenticidad e integridad.

X. *PRESERVACIÓN DE LOS DATOS Y VOLCADO DE LA INFORMACIÓN*

De conformidad con el art. 230.2 LOPJ, resulta necesario asegurar la autenticidad [garantiza la fuente de la que proceden los datos (51)] y la integridad [el activo de información no ha sido alterado de manera no autorizada (52)] de la prueba electrónica incorporada al proceso, de tal manera que quede garantizado que la sometida al tribunal de enjuiciamiento es la misma que la que fue incautada o aprehendida. La cadena de custodia adopta, pues, una serie de singularidades cuando se aplica a las pruebas electrónicas. Resulta conveniente abordar estas singularidades a través de su regulación y/o protocolización: aportará certidumbre a la actuación de los distintos sujetos del sistema penal y reducirá el margen error en sus actuaciones, limitando el riesgo de contaminación o alteración de la autenticidad e integridad de las pruebas (53) .

No han de surgir especiales problemas cuando se trata de la incorporación al proceso del propio dispositivo electrónico, ya sea por quedar bajo la custodia del Secretario Judicial o por quedar en posesión de la Policía Judicial u organismo especializado a disposición del Juez. Sin embargo son más complejos los casos en los que es necesario realizar una copia o clonado de la información del dispositivo (volcado de datos) para la realización de un análisis en el seno de una pericial.

El volcado consiste en la realización de una copia espejo o bit a bit de la información original (54) en el mismo lugar en el que se encuentra el dispositivo o en una diligencia posterior. El principal problema radica en la presencia del Secretario Judicial durante la práctica del volcado porque, aunque la misma se ha venido exigiendo por la práctica de los tribunales, también es cierto que existen varias sentencias del Tribunal Supremo (SSTS 1599/1999 de 15 de noviembre, 256/2008 de 14 de mayo y 480/2009 de 22 de mayo) que no la consideran necesaria porque «ninguna garantía podría añadirse con la presencia del Secretario judicial al que no se le puede exigir que permanezca inmovilizado durante la extracción y ordenación de los datos, identificando su origen y procedencia» (STS 480/2009 caso *Ekin-Kas-Xaki).*

El volcado ante el Secretario Judicial resulta conveniente para garantizar la preservación de la información, pero no es requisito de validez de la prueba de tal manera que su ausencia no determina su nulidad; el practicado sin su presencia no es una prueba preconstituida, sino que ha de llevarse al juicio oral por otras vías, especialmente mediante la declaración de los agentes que realizaron el volcado que será valorada por el tribunal de enjuiciamiento. Cabe destacar que existen medios tecnológicos que permiten que el Secretario Judicial garantice la autenticidad e integridad de la fuente de prueba; siendo de gran utilidad el hash, es decir, un algoritmo que permite afirmar que los datos que se encontraban en el dispositivo en el momento de su ocupación no han sido objeto de manipulación posterior (55) . Por último, los agentes que realicen el volcado usarán elementos técnicos para garantizar la autenticidad e integridad de los datos, que habrán de documentarse para su incorporación al proceso, por lo que es relevante la homologación de equipos y programas.

(1)

Carolina SANCHÍS CRESPO define prueba electrónica o en soporte electrónico como «aquella información contenida en un dispositivo

electrónico a través del cual se adquiere el conocimiento de un hecho controvertido, bien mediante el convencimiento psicológico, bien al fijar este hecho como cierto atendiendo a una norma legal»; en «La prueba en soporte electrónico», dentro de la obra colectiva «Las Tecnologías de la Información y de la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio», Ed. Thomson Reuters Aranzadi, Navarra, 2012, pág. 713.

Ver Texto

(2)

Se tiene en cuenta la concepción amplia que se contiene en el Convenio de Budapest sobre Ciberdelincuencia de 23 de noviembre de 2001 (Instrumento de Ratificación por España en BOE de 17 de septiembre de 2010) que define «datos informáticos» de la siguiente forma: «se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función».

Ver Texto

(3)

El Anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia define «medio electrónico» como «mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones; incluyendo cualesquiera redes de comunicación abiertas o restringidas como Internet, telefonía fija y móvil u otras».

Ver Texto

(4)

Afirma Francesco CARNELUTTI que «el uso de la palabra prueba se limita a los procedimientos instituidos por el juez para la comprobación de los hechos controvertidos»; en «La prueba civil», Ediciones Depalma, Buenos Aires, 1982, pág. 43.

Ver Texto

(5)

Los distintos elementos de cualquier tipo de la infracción penal pueden resultar acreditados mediante evidencias que se encuentran en dispositivos electrónicos. Los autores de los delitos se aprovechan de las posibilidades que les ofrecen las tecnologías para facilitar la realización del hecho punible y su impunidad, especialmente en los casos de criminalidad organizada. Asimismo, en la comisión de delitos resulta cada vez más frecuente la presencia de dispositivos de naturaleza electrónica: teléfonos móviles, smartphones, tabletas, dispositivos USB y otros muchos accesibles en el mercado ordinario y de uso cotidiano. Véase Juan SALOM CLOTET, «Incidencias de la nueva regulación en la investigación de los delitos cometidos a través de medios informáticos», dentro de «La protección de datos en la cooperación policial y judicial», editado por la Agencia Española de Protección de Datos y Ed. Thomson Aranzadi, 2008, pág. 140; y Manuel DÍAZ MARTÍNEZ, «El factor criminógeno de las TIC», dentro de la obra colectiva «El proceso penal en la sociedad de la información», Ed. LA LEY, págs. 534 y ss.

Ver Texto

(6)

El Convenio de Budapest sobre Ciberdelincuencia fija el ámbito de

aplicación de sus disposiciones procesales no solamente para los procedimientos por delitos cometidos por medio de un sistema informático, sino también para la obtención de pruebas electrónicas de cualquier delito (art. 14.2).

Ver Texto

(7)

Julio BANACLOCHE PALAO, «La prueba en el proceso penal», dentro de la obra «Aspectos fundamentales del Derecho Procesal Penal», Ed. LA LEY, 2.ª ed., Madrid 2011, pág. 273.

Ver Texto

(8)

En este marco nos encontramos con el concepto de «documento electrónico» cuando la información se recoge en un soporte electrónico según un formato determinado y que sea susceptible de identificación y tratamiento diferenciado. En este sentido es necesario tener en cuenta la definición de documento electrónico que se contiene en el Anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia: «información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado». Raquel CASTILLEJO MANZANARES recuerda que «es un documento electrónico un documento de texto, una hoja de cálculo, una imagen digitalizada, un fichero de sonido, un vídeo digitalizado o un registro o conjunto de registros dentro de una base de datos», «Medios probatorios», dentro del libro Hacia un nuevo proceso penal. Cambios necesarios, ed. 1.ª, Ed. LA LEY, Madrid, octubre 2010.

Ver Texto

(9)

María Luisa GARCÍA TORRES, «La tramitación electrónica de los procedimientos judiciales, según ley 18/2011, de 5 de julio reguladora del uso de las tecnologías de la información y la comunicación en la administración de justicia. Especial referencia al proceso civil», Revista Internacional de Estudios de Derecho Procesal y Arbitraje, www.riedpa.com, núm. 3-2011.

Ver Texto

(10)

Véase también Corazón MIRA ROS, «El expediente judicial electrónico», Ed. Dykinson SL, Madrid 2010, pág. 18.

Ver Texto

(11)

El art. 19 de Convenio de Budapest se refiere al registro y confiscación de datos informáticos contenidos: en «un medio de almacenamiento de datos en el que puedan almacenarse datos informáticos»; y en «un sistema informático o una parte del mismo, así como los datos informáticos almacenados en él»; según el art. 1 del Convenio, por sistema informático cabe entender «todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa».

Ver Texto

(12)

MINISTERIO DE JUSTICIA, «Propuesta de texto articulado de Ley de Enjuiciamiento Criminal, elaborada por la Comisión Institucional creada por Acuerdo del Consejo de Ministros de 2 de marzo de 2012», editado por el Ministerio de Justicia, Madrid, 2013.

Ver Texto

(13)

European Network of Forensic Science Institutes: http://www.enfsi.org

Miembros de España: Criminalistic Service of the Civil Guard, Madrid; Forensic Science Unit. Basque Country Police.Spain. (FSU), Erandio; General Commissary of Scientific Police (GCSP), Madrid; National Institute of Toxicology and Forensic Science, Madrid; Scientific Police Division (CME), Sabadell

Ver Texto

(14)

Así se manifiesta la STC 115/2013, de 9 de mayo, en referencia a los teléfonos móviles pero que resulta de aplicación a otros dispositivos electrónicos. Véase el comentario a esta sentencia del TC de Isabel GUAJARDO PÉREZ, «Agenda del teléfono móvil y registro de llamadas. Doctrina sobre el contenido del derecho de intimidad y al secreto de comunicaciones», Diario LA LEY, núm. 8135, Sección Jurisprudencia del Tribunal Constitucional, 26 de julio de 2013.

Ver Texto

(15)

Sobre el concepto de comunicación, véase José Luis RODRÍGUEZ LAINZ, «En torno al concepto de comunicación protegida por el art. 18.3 de la Constitución», Diario LA LEY, núm. 8142, Sección Doctrina, 5 de septiembre de 2013.

Ver Texto

(16)

Manuel MARCHENA GÓMEZ destaca que «de ordinario, en cualquier programa de gestión de correo electrónico se agolpan mensajes recibidos y abiertos, no abiertos y eliminados sin abrir»; y añade posteriormente que «resultará mucho más seguro estimar que el acceso a esos mensajes, ya sean los que se hallen en el servidor pendientes de descarga como los que se encuentren almacenados en el ordenador del sospechoso, abiertos o no, requiere una resolución jurisdiccional ajustada a las exigencias constitucionales y legales que legitiman la injerencia en el secreto de las comunicaciones, "Dimensión jurídico-penal del correo electrónico"», Diario LA LEY, núm. 6475, Sección Doctrina, 4 de mayo 2006, Ref. D-114.

Ver Texto

(17)

Sobre este derecho véase Pablo Lucas Murillo de la Cueva, «Los derechos fundamentales al secreto de las comunicaciones y a la autodeterminación informativa», dentro de la obra «Derecho Procesales Fundamentales», Manuales de Formación Continuada, 22, editado por el Consejo General del Poder Judicial, Madrid, 2005, págs. 161 y ss.

Ver Texto

(18)

Raquel BONACHERA VILLEGAS, «El registro de archivos informáticos: una cuestión necesitada de regulación», en Revista General de Derecho Procesal 27(2012), pág. 11.

Ver Texto

(19)

Véase Juan Luis MARONDA FRUTOS y María Isabel TENA FRANCO, «El comiso y secuestro de objetos para fines probatorios no cautelares», Cuadernos de Derecho Judicial, volumen sobre «Medidas restrictivas de derechos fundamentales», editado por el Consejo General del Poder Judicial, Madrid, 1996, págs. 209 y ss.; y M.ª Paloma BELA y RODRÍGUEZ DE ZABALETA, «Conservación de los bienes y objetos afectos a las actuaciones judiciales: piezas de convicción, instrumentos del delito, cuerpo del delito. Destino legal de las piezas. Destrucción bajo la fe del Secretario», Estudios Jurídicos Secretarios Judiciales, editado por el Centro de Estudios Jurídicos de la Administración de Justicia, Madrid, 2000, págs. 373 y ss.

Ver Texto

(20)

Luis Alfredo DE DIEGO DÍEZ, «Control judicial sobre las piezas de convicción: la puesta a disposición judicial», Diario LA LEY, núm. 6196, Sección Doctrina, 23 de febrero de 2005.

Ver Texto

(21)

En la definición de estas tres categorías se sigue la exposición de Luis Alfredo DE DIEGO DÍEZ, «Ocupación, conservación y destrucción de las

piezas de convicción», Ed. Tirant lo Blanch, Valencia, 2005, págs. 18 y 19.

Ver Texto

(22)

Véase Joaquín DELGADO MARTÍN, «La resolución judicial de entrada y registro en lugar cerrado», Actualidad Penal, núm. 47, Sección Doctrina, 2001, Ref. XLVII, pág. 1125, tomo 3, Ed. LA LEY; y Julio BANACLOCHE PALAO, «Las diligencias de investigación restrictivas de los derechos fundamentales», dentro de la obra Aspectos fundamentales del Derecho Procesal Penal, Ed. LA LEY, 2.ª ed., Madrid, 2011, págs. 178 y ss.

Ver Texto

(23)

Se trata de un concepto amplio que se deduce de los arts. 546 y 547 LECrim. Véase José Antonio DÍAZ CABIALE, «La admisión y práctica de la prueba en el proceso penal», editado por el CGPJ, Madrid, 1992, pág. 157.

Ver Texto

(24)

Sobre el concepto de domicilio y el casuismo jurisprudencial, véase Javier M. CUCHI DENIA y Cristina BASOLS CAMBRA, «El domicilio como objeto de la diligencia de entrada y registro: su concepto y casuística», en Revista General de Derecho Procesal 28(2012).

Ver Texto

(25)

Vid. Jaime VEGAS TORRES, Presunción de inocencia y prueba en el proceso penal, Ed. LA LEY, Madrid, 1993, pág. 364.

Ver Texto

(26)

La STS 545/2011 de 27 de mayo, en alusión a la entrada en un local sin actividad mercantil y destinado a almacén, afirma expresamente que «ni toda entrada y registro en un lugar cerrado exige la autorización judicial, ni los locales comerciales o almacenes que no constituyen morada de una persona gozan de la tutela constitucional del art. 18.2 citado, sin que requieran, en consecuencia, para la entrada y registro en ellas de las mismas formalidades procesales que se imponen a los registros domiciliarios (STS 8-7-94)».

Ver Texto

(27)

Carmen DURÁN SILVA, después de repasar las diferentes posturas doctrinales sobre la necesidad de autorización en estos supuestos, opina que «la Policía Judicial podría proceder a la entrada y registro de dichos lugares sin precisar autorización judicial, salvo aquellas partes reservadas de los mismos que, por ejemplo, por estar destinadas a los libros de contabilidad, sería imprescindible obtener autorización judicial para el desarrollo del registro»; en «La diligencia de entrada y registro: su necesaria adaptación a la realidad actual», dentro del libro La reforma del proceso penal, Ed. LA LEY, Madrid, 2011.

Ver Texto

(28)

Sin perjuicio de que pueda afectar a la intimidad el registro de alguno de los elementos que se encuentren en el lugar cerrado.

Ver Texto

(29)

La STS 545/2011 de 27 de mayo, niega el carácter de prueba preconstituida a una diligencia de entrada en un almacén por la no intervención de los dos imputados presos ni sus letrados (falta de contradicción), pero admite su acceso al proceso a través de las declaraciones en juicio de los policías.

Ver Texto

(30)

No hay que olvidar los supuestos de flagrancia o de consentimiento del titular del domicilio, expreso o tácito, que plantean cuestiones específicas que exceden del objeto de este trabajo. Y por la misma razón tampoco vamos a entrar en el análisis de los problemas derivados del respeto al derecho de defensa de la persona investigada, ni en los relativos a la presencia/ausencia del Secretario Judicial. Vid. Carmen FIGUEROA NAVARRO, «La obtención de pruebas mediante la entrada y registro en domicilio», La Ley Penal núm. 91, Sección Estudios, marzo 2012.

Ver Texto

(31)

Jaime VEGAS TORRES, «Prueba ilícita en particular (II): la ilicitud de la

entrada y registro en lugar cerrado y sus consecuencias», Cuadernos de Derecho Judicial, volumen dedicado a «La prueba en el proceso penal II», editado por el Consejo General del Poder Judicial y la Escuela Judicial, Madrid, 1996, págs. 362 y 362.

Ver Texto

(32)

En principio, se trataría de una exclusión automática de toda prueba que tenga relación «natural» con una diligencia de entrada y registro ilícita (por vulnerar un derecho fundamental), sin consideración de las circunstancias concurrentes en el caso concreto. Sin embargo, la jurisprudencia ha optado por una restricción a través de la denominada «conexión de antijuridicidad»: una prueba refleja tendrá validez siempre y cuando se considere que es jurídicamente independiente de la prueba de la que deriva. Se viene a recibir en el Derecho español la doctrina anglosajona de la independent source o fuente independiente. Sobre la recepción del Derecho anglosajón en la materia, véase Jesús FERNÁNDEZ ENTRALGO, «Las reglas del juego. Prohibido hacer trampas: la prueba ilegítimamente obtenida», Cuadernos de Derecho Judicial, volumen dedicado a «La prueba en el proceso penal II», editado por el Consejo General del Poder Judicial y la Escuela Judicial, Madrid, 1996, págs. 57 y ss. Véase también José María ASENCIO MELLADO, «Prueba ilícita: declaración y efectos», Revista General de Derecho Procesal 26 (2012); y María MARCOS GONZÁLEZ, «Doctrina constitucional sobre la prueba ilícita: discrepancias interpretativas», La Ley Penal, núm. 88, Sección Estudios, diciembre 2011, Ed. LA LEY.

Ver Texto

(33)

Teresa SÁNCHEZ NÚÑEZ, «Jurisprudencia del Tribunal Constitucional

sobre el uso de las nuevas tecnologías en la investigación penal», Cuadernos de Derecho Judicial, volumen sobre «Los nuevos medios de investigación en el proceso penal. Especial referencia a la tecnovigilancia», editado por el Consejo General del Poder Judicial, Madrid, 2007, pág. 271

Ver Texto

(34)

Entiende Raquel CASTILLEJO MANZANARES que «el procedimiento adecuado en estos supuestos, esto es, cuando se trate de la inspección o recogida de dispositivos y soportes de almacenamiento masivo de datos, es que la autorización judicial debería contener expresamente su práctica y sobre qué soportes se ha de realizar. Aunque cabrá que, por un lado, sea imposible llevar a cabo una previsión específica de lo que pueda ser hallado, en cuyo caso basta la mención genérica a la inspección y recogida de dichos soportes durante la diligencia, siempre que aparezcan motivos racionales para creer que pueden contener alguna información sobre el hecho investigado. Por otro lado, puede resultar imposible hacer constar en la autorización todas aquellas circunstancias que puedan acaecer y servir para el buen fin de la investigación, supuesto en el que la policía, no contradiciendo la autorización, podrá llevar a cabo las actuaciones que sirviendo al buen fin de la investigación, y respondiendo a circunstancias imprevistas, puedan ser convalidadas posteriormente por el Juez»; en «Medios Probatorios», obra citada.

Ver Texto

(35)

Raquel BONACHERA VILLEGAS entiende que «la orden ha de mencionar los dispositivos que se pretenden recoger y examinar, y razonar, que en

ellos se encuentra información sobre el hecho investigado»; en «El registro de archivos informáticos…», obra citada, pág. 6.

Ver Texto

(36)

Véase Juan Carlos ORTIZ PRADILLO, «Nuevas medidas tecnológicas de investigación criminal para la obtención de la prueba electrónica», dentro de la obra colectiva El proceso penal en la sociedad de la información, Ed. LA LEY, pág. 276.

Ver Texto

(37)

Raquel CASTILLEJO MANZANARES estima que «si los datos se introducen en un dispositivo de memoria sito en la vivienda, sobre los mismos recaerá la cobertura del art. 18.2 CE, pero si los datos se guardan en el alojamiento contratado con un proveedor de servicios, dicha norma no resultará de aplicación, por mucho que la información se refiera a la vida más íntima de la persona, se proteja de la curiosidad de terceros mediante las más avanzadas técnicas disponibles, se haya creado y se acceda a ella exclusivamente en y desde el hogar»; en «Medios probatorios», obra citada, pág. 25.

Ver Texto

(38)

El art. 350.3 del PLECrim.-2013 que «cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del Ministerio Fiscal

quien podrá solicitar del Tribunal de Garantías una ampliación de los términos del registro».

Ver Texto

(39)

Juan Carlos ORTIZ PRADILLO, «Nuevas medidas tecnológicas…», obra citada, pág. 289.

Ver Texto

(40)

«Troyano» es un programa que, una vez que se ejecuta, permite a quien realiza la infección controlar la máquina anfitriona. Entre otras, puede tener las siguientes finalidades: acceso y sustracción de información personal, borrado o manejo de archivos, instalación de otros programas (maliciosos o no), reinicio o apagado del equipo.

Ver Texto

(41)

Véase Juan Carlos ORTIZ PRADILLO, «Propuestas para la lucha contra el cibercrimen: la obtención transfronteriza de prueba electrónica en la Unión Europea», en Revista General de Derecho Procesal 20(2010), pág. 6. Este autor defiende que este tipo de medidas «proporciona a las autoridades la posibilidad de acceder de forma rápida a una valiosa fuente de prueba (la información almacenada en el equipo informático), pero deben establecerse legalmente las circunstancias, requisitos y límites bajo los cuales estos registros remotos (transfronterizos o no) resultarán admisibles»; obra citada, pág. 9.

Ver Texto

(42)

Juan Carlos ORTIZ PRADILLO, «Nuevas medidas tecnológicas.», obra citada, pág. 290.

Ver Texto

(43)

Eloy VELASCO NÚÑEZ, «ADSL y troyanos: intervención de sus datos y telecomunicaciones en la investigación penal», La Ley Penal, núm. 82, mayo 2011, págs. 22 y 23.

Ver Texto

(44)

Siguiendo a Juan Carlos ORTIZ PRADILLO, cabe tener en cuenta que en el teléfono intervenido se puede implantar un chip o instalar de forma remota un software para que, desde otro terminal, se pueda monitorizar toda la gestión del original, servir de estación de escucha, conocer su ubicación, o activar el micrófono del teléfono replicado sin necesidad de que éste se encuentre encendido; en «Nuevas medidas tecnológicas de investigación…», obra citada, pág. 296.

Ver Texto

(45)

Hay autores que se han manifestado expresamente a favor de la admisibilidad, como Eloy VELASCO NÚÑEZ, «ADSL y troyanos…», obra

citada, pág. 24. Juan Carlos ORTIZ PRADILLO estima que los tribunales «han colmado jurisprudencialmente las importantes lagunas de nuestro Ordenamiento y han legitimado el uso de nuevas fórmulas de investigación, sobre la base de una legislación anquilosada en el pasado»; añadiendo posteriormente que «como mal menor y para el supuesto de que se lleve a cabo dicha interpretación jurisprudencial integradora que admita la posibilidad de realizar un registro on line, ya advertimos en su momento los requisitos que deberían cumplirse», resumiéndolos a continuación; en «Nuevas medidas tecnológicas.», obra citada, págs. 299 y 304.

Ver Texto

(46)

El subrayado es mío.

Ver Texto

(47)

El art. 350.4 PLECrim. 2103 establece que «el registro remoto sólo podrán ser autorizado cuando los datos se encuentren almacenados en un sistema informático o una parte del mismo situado en territorio sobre el que se extienda la jurisdicción española. En otro caso, se instarán las medidas de cooperación judicial internacional en los términos establecidos por la Ley, los Tratados y Convenios internacionales aplicables y el derecho de la Unión Europea».

Ver Texto

(48)

Véase Joaquín DELGADO MARTÍN, «Emisión de una Decisión de

Embargo Preventivo de Bienes o Aseguramiento de Pruebas en el ámbito de la Unión Europea», dentro de la obra «La nueva Ley para la eficacia en la Unión Europea de las resoluciones de embargo y aseguramiento de bienes en procedimientos penales», Estudios de Derecho Judicial, 117, editado por CGPJ, Madrid, 2007, págs. 253 y ss.; y Eloy VELASCO NÚÑEZ, «Cuestiones procesales relativas a la investigación de los delitos telemáticos», Cuadernos de Derecho Judicial, volumen sobre «Delitos contra y a través de las nuevas tecnologías. ¿Cómo reducir su impunidad?», editado por el CGPJ, Madrid, 2006, págs. 269 y ss.

Ver Texto

(49)

Dependiendo del caso podrán ser aplicables, entre otros, el Convenio de 29 de mayo de 2000 relativo a la asistencia judicial en materia penal entre Estados miembros de la UE, el Convenio relativo al blanqueo, seguimiento, embargo y decomiso de los productos del delito de 8 de noviembre de 1990, el Convenio de ONU contra el tráfico ilícito de estupefacientes y sustancias psicotrópicos de 20 de diciembre de 1988, o el Convenio de ONU contra la delincuencia organizada transnacional, firmado en Palermo el 13 de diciembre de 2000. Para más información véase www.prontuario.org .

Ver Texto

(50)

Raquel CASTILLEJO MANZANARES entiende que «en el supuesto de que sea introducido por las partes en el proceso, la normativa resulta escasa en lo relativo a la aportación de la prueba documental y demás pruebas de convicción, por eso opinamos, como lo hace Moreno Catena, que debe aplicarse por analogía el régimen legal previsto en el marco de los

artículos de previo pronunciamiento para la prueba documental —arts. 666 y ss. LECrim.—»; en «Medios probatorios», obra citada, pág. 26.

Ver Texto

(51)

Según definición contenida en el Anexo de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia.

Ver Texto

(52)

Según definición contenida en el Anexo de la Ley 18/2011.

Ver Texto

(53)

Véase Carmen FIGUEROA NAVARRO, «El aseguramiento de las pruebas y la cadena de custodia», La Ley Penal, núm. 84, Sección Estudios, julio 2011.

Ver Texto

(54)

Juan SALOM CLOTET, «Incidencias…», obra citada, pág. 145.

Ver Texto

(55)

Afirma Eloy VELASCO NÚÑEZ que «cada vez más las nuevas tecnologías —grabaciones, videoconferencias, clonados con resumen digital hash, etc.— suplen la por otra parte innecesaria presencia continuada del Secretario judicial en la práctica de algunas onerosas diligencias procesales»; en «Correo electrónico, SMS y «virus troyanos», Cuadernos Digitales de Formación 22 – 2009, Consejo General del Poder Judicial, nota 31.

Ver Texto