Revista Electrónica de Estudios Penales y de la Seguridad
ISSN: 2531-1565

RECENSIÓN

Reflexiones sobre *Investigación y prueba mediante el uso de las nuevas tecnologías*, a propósito de "La obtención de evidencia digital en un marco de cooperación internacional", de María Julia Solari

Arturo Álvarez Alarcón
Catedrático de Derecho Procesal
Universidad de Cádiz (España)

1. Son muy numerosas las cuestiones que se plantean por María Julia Solari en su trabajo "La obtención de evidencia digital en un marco de cooperación internacional", que difícilmente pueden ser tratadas en un breve artículo, no sólo por la enjundia que cada una de ellas encierra, sino también por la muy diferente naturaleza de cada una de ellas.

2. Antes de nada, y como cuestión previa, conviene señalar que el empleo de la expresión evidencia es más propio de los ordenamientos y estudios jurídicos del *common law*, más que los del *civil law*, y especialmente, los que se producen en el ámbito latino e iberoamericano. Probablemente ello sea producto de la concreta bibliografía consultada.

3. La "obtención de evidencia", que se contiene ya en el título, nos induce a pensar que se trata de un trabajo fundamentalmente procesal. En el texto se hace mención indistintamente a los procesos penales y también a los civiles, aunque luego se centra esencialmente en el enjuiciamiento de los delitos, incluso aportando algún concreto ejemplo (extraído de la jurisprudencia norteamericana). Es necesario discernir entre ambos ámbitos, porque los intereses y principios que se encuentran afectados en uno y otra clase de procesos provocará diferentes conclusiones en relación con el estudio de la prueba y las nuevas tecnologías, particularmente en lo que se refiere a las posibilidades de su obtención y aportación al proceso. Dado que el texto se refiere esencialmente a cuestiones de carácter penal (además del ejemplo utilizado, se habla en numerosas ocasiones de "delitos", de "delitos informáticos", de "investigaciones criminales", "investigaciones de delitos", "investigación y determinación de delitos", etc., las observaciones que aquí se hacen se refieren fundamentalmente a esta clase de procesos[1].

4. Menciona el título también a la cooperación internacional. Pero es breve la atención que presta a este asunto, que apenas va más allá de la referencia al Convenio de Budapest[2]. Es cierto que también refiere (nota 21) el marco interamericano de asistencia judicial mutua, pero no va más allá de una mera relación de convenios, acuerdos y tratados bilaterales, tomados de una de las obras consultadas, que tiene carácter internacional-regional. Realmente, el análisis de todo

[1] Cuando la autora se refiere a los aspectos civiles, o lo relaciona con la víctima (sic) o con la responsabilidad civil y penal, con lo que parece que está pensando en supuestos de responsabilidad civil derivada de la penal; por consiguiente, siempre es el enjuiciamiento penal el objeto de su atención.

[2] Con el fin de completar la información de la autora, se señala que el conocido como Convenio de Budapest es un Convenio sobre la Ciberdelincuencia, aprobado por el Consejo de Europa en Budapest el 23 de noviembre de 2001, (https://www.oas.org/juridico/english/cyb_pry_convenio.pdf), conteniendo aspectos de Derecho Penal y también de Derecho Procesal

ello excedería con mucho la extensión de un único artículo, pues, además, debería abordar también el estudio de otros textos internacionales. Particularmente interesante sería acudir a los producidos en el ámbito de la Unión Europea, que desde el año 2014 cuenta con la *Orden Europea de Investigación*[3], que constituye un magnífico ejemplo de cooperación judicial internacional[4]. Por ello, tampoco se va a hacer mención aquí a estas cuestiones de carácter internacional, ni a las relativas a la jurisdicción ni a la soberanía de los Estados.

5. Sí que, en cambio, merece hacer una reflexión sobre los aspectos procesales que se suscitan en relación con el uso de las nuevas tecnologías como medio de investigación y prueba de los delitos. En su trabajo aflora en algún momento alguna mención al ordenamiento argentino, pareciendo que constituye su referencia. Se comprende así que hable de la falta de regulación de esta materia. En efecto, sostiene que esta materia carece de regulación y que se está acudiendo a la aplicación analógica de ciertos preceptos del Código Procesal Penal de la Nación Argentina, sobre intervención de comunicaciones, interceptación de correspondencia, allanamientos, secuestros y requisas. Y la mención a estas normas argentinas se hace para plantear a medias unos interrogantes sobre los que dice que "puede presumirse que la aplicación de estas normativas por vía analógica puede llevar muchas veces a soluciones que no son apropiadas". Pero no dice por qué son inapropiadas. "En ese sentido, al no existir reglas claras pueden darse tanto supuestos de enormes invasiones a derechos individuales y en otros se puede decidir cerrar investigaciones legítimas en sustento a una idea de privacidad cuya definición quedó desactualizada". Pero no explica por qué ocurre esto y que es, precisamente, lo más relevante de las cuestiones que plantea la autora sobre la investigación y prueba (o "evidencia") en el proceso penal por medio de las nuevas tecnologías.

6. Nos encontramos ante la investigación y prueba de hechos que se realizan en el "ciberespacio" y que por sí mismos pueden integrar el tipo delictivo, pero también otros que de alguna manera permiten probar el hecho criminal o la autoría del mismo. No se trata sólo de los delitos informáticos, ni tampoco de los delitos de injurias y calumnias por medios telemáticos o cibernéticos, sino también de otros muchos en los que los sujetos que los cometen utilizan las nuevas tecnologías para su comisión, o, simplemente, para su vida ordinaria.

7. Un adecuado planteamiento del recurso a estos medios conduce, necesariamente, reflexionar sobre la afectación que pueda producirse con ellos en los derechos fundamentales de la persona. A ello se refiere también la autora, bajo la denominación de "interpretación de principios constitucionales en la era digital", remitiéndose a los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones. Aquí convendría destacar

[3] Directiva 2014/41/CE del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativa a la orden europea de investigación en materia penal (https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32014L0041)

[4] La orden europea de investigación crea un régimen único para la obtención de pruebas, aunque establece normas adicionales para determinados tipos de medidas como el traslado temporal de detenidos, las comparecencias por teléfono, videoconferencia u otros medios de transmisión audiovisual, la obtención de información relacionada con cuentas o transacciones bancarias o financieras, las entregas vigiladas o las investigaciones encubiertas y la intervención de telecomunicaciones con asistencia de otro Estado miembro.

adecuadamente cuales son los derechos fundamentales que pueden verse vulnerados en el caso de la persecución procesal de los delitos, que no es lo mismo que la mera vigilancia de las comunicaciones que tiene carácter preventivo. Por tanto, bajo la excusa de la seguridad nacional se pueden adoptar ciertas medidas de vigilancia, de carácter general; pero no es el mismo supuesto en el que se trata de la persecución de un delito concreto que ya se ha cometido o que podría haber sido cometido. En el primer caso, la actitud vigilante del Estado, que a todos puede afectar de modo inmediato, debe ser sometida a rígido control para evitar que los ciudadanos nos encontremos abocados a una suerte de "gran hermano". Cautela que igualmente debe extenderse sobre otras conductas de entes privados, pero que no viene al caso ahora. Distinto es el caso en el que se persigue un concreto delito, porque en este supuesto el fundamento no es una hipotética comisión de conducta delictiva, sino que ésta en efecto se ha cometido; y con la medida que se adopte no se afectará de modo concreto a la generalidad de los ciudadanos sino a aquél o aquellos que se encuentren íntimamente ligados al hecho criminal.

8. ¿Qué debemos entender por nuevas tecnologías, a estos efectos? No lo es sólo Internet o el ciberespacio, si es que ambos términos pudieran ser coincidentes; también lo son los instrumentos con los que se accede a Internet, los cuales, a su vez, aunque no estén conectados, también constituyen una nueva tecnología, en el sentido de no previsto por el ordenamiento: ordenadores, teléfonos, etc. Incluso, ahora que se nos amenaza con la llegada de las "casas inteligentes", también lo serán los aparatos domésticos. No es lo característico de ellos que se pueda obtener una información accediéndolos sin perturbar al titular (la autora señala el ejemplo de los "gusanos" informáticos), pues ello podría ocurrir también, por ejemplo, si se penetra en un domicilio sin conocimiento del titular, o se graban sus imágenes o conversaciones. Lo peculiar es que se trata de una tecnología que almacena una ingente cantidad de datos que sólo pueden visualizarse o percibirse por los sentidos mediante el uso de unos artefactos especiales, y que permite la comunicación inmediata merced a dichos ingenios. La información y la comunicación se producen de modo sencillo para los ciudadanos, sin perjuicio de que en su "interior" se produzcan multitud de operaciones y se generen datos y "rastros" que pueden ser conocidos y descifrados por los expertos.

Pero, lo que es relevante para el Derecho es que mediante estas nuevas tecnologías se produce el almacenamiento de información de los ciudadanos y la comunicación entre ellos. Por tanto, si alguien penetra en estos ámbitos que le deben ser ajenos, se podrá ocasionar una quiebra de los derechos fundamentales a la intimidad y al secreto de las comunicaciones.

Y esto puede tener lugar accediendo a un computador, a un teléfono móvil, a una "tablet", pero también a las cuentas de correo, Facebook, etc., alojadas en algún servidor.

9. El ciberespacio… No es absolutamente intangible, por más que no podamos tocarlo, verlo, olerlo… El ciberespacio como conjunto de datos existe electrónica y magnéticamente, alojado o fluyendo entre ordenadores. No se trata ahora de plantear cuestiones sociológicas y económicas sobre este fenómeno, sino algo más concreto, que es el acceso a ese conjunto de datos, almacenados o fluyentes,

con los fines de persecución de un delito. Se haga como se haga, ese acceso puede afectar a los derechos fundamentales de personas concretas.

Por consiguiente, para que el acceso a una información o a unas comunicaciones, almacenadas o producidas mediante el uso de las nuevas tecnologías, pueda ser útil en un concreto proceso penal, es necesario que se lleve a cabo conforme a ciertas reglas, generalmente admitidas ya por la literatura procesal, que son las que se echan de menos en el trabajo de Doña María Julia Solari. Se trata de las condiciones que impone el denominado juicio o principio de proporcionalidad sobradamente conocido y que requiere:

- Finalidad legítima: La existencia de un fin constitucionalmente legítimo. Es legítimo el fin cuando lo que se pretende es la persecución de los delitos y sus autores, en aplicación de las leyes penales y procesales

- *Principio de legalidad*: La medida limitativa del derecho fundamental debe estar prevista en la ley. Esta condición es muy importante, pues estamos en un ámbito en el que la analogía no es admisible. Al menos no lo es para introducir una conducta que afecta a los derechos fundamentales, aunque pueda serlo para la regulación de algún aspecto concreto. Por tanto, no puede ser admisible la actuación que nao haya sido expresamente contemplada por la ley. Así, por más que pueda quererse asimilar a la intervención de la correspondencia postal, la interceptación de la comunicación por correos electrónicos o whatsapp necesita que el legislador la haya previsto.

- *Autorización judicial motivada.* La regla general debe ser la de que sólo se puedan adoptar las medidas que atentan contra los derechos fundamentales si concurre una resolución judicial motivada que la autoriza. Esto debe ocurrir igualmente con las nuevas tecnologías. Cabe señalar aquí que en ordenamiento español la Constitución impone que así se haga únicamente respecto de las comunicaciones, pero no respecto de la intimidad, por lo que la ley puede permitir que la policía judicial practique las actuaciones autorizadas por la ley sin esperar a la autorización del juez, por más que atenten contra los derechos fundamentales. No obstante, aunque la Constitución no lo requiera, la reciente reforma ya citada de 2015, impone que para que la policía judicial pueda penetrar en el ámbito de la intimidad de una persona, se precisa autorización judicial.

- *Principio de proporcionalidad*: Esta regla o principio se desarrolla en tres mandatos:

- *Juicio de idoneidad*: Que la actuación autorizada y practicada sea útil para la consecución del objetivo propuesto

- *Juicio de necesidad*: Que no exista otra medida menos perjudicial para el derecho afectado y que permita su obtención con igual eficacia.

- *Juicio de proporcionalidad*: Que obliga a sopesar si de la práctica de la actuación y el consiguiente perjuicio para el derecho fundamental, se obtienen más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto. En relación con esto, la violación de un derecho fundamental no es una cuestión meramente cuantitativa, sino que lo es esencialmente cualitativa. La intervención inadecuada de una sola y breve comunicación ya es suficiente para que se

haya provocado la quiebra del derecho fundamental y, por tanto, su nulidad a efectos procesales.

Este juicio de proporcionalidad se encuentra totalmente admitido en el ámbito de la Unión Europea por numerosas resoluciones del Tribunal de Justicia de la Unión Europea y por los tribunales ordinarios de los diferentes Estados miembros. En el ámbito español, ocurre otro tanto con el Tribunal Supremo y con el Tribunal Constitucional[5].

10. La práctica de los actos de investigación precisa una regulación que alcance numerosos aspectos para evitar las dudas abundantes que en la misma se pueden y suelen suscitar y que luego tienen relevancia a la hora del enjuiciamiento, en el momento de ser valoradas. Así, la autora se preocupa en una ocasión por el denominado hallazgo casual y entiende, siguiendo al autor que cita, que "[e]n ese contexto ningún hallazgo será casual, ni producto de la aplicación simple de los sentidos y solo puede tener lugar al requisar la totalidad de los datos de un dispositivo" y concluye afirmando que "se observa claramente que los datos obtenidos como consecuencia de un registro digital no pueden ser regulados de la misma forma que los de un registro físico; debiéndose ponderar en el caso la protección de garantías, por un lado, y la eficiencia de las investigaciones, por otro".

Quizás sea exagerada la afirmación sobre que ningún hallazgo puede ser casual en esta materia. Así, por ejemplo, es conocido en la jurisprudencia española[6], el supuesto del descubrimiento casual de pornografía infantil. Se trata de una ocasión en la que el propietario de un equipo informático acude al técnico para que lo repare y éste, al comprobar el funcionamiento correcto toma al azar fotografías y vídeos de un archivo, descubriendo así el contenido pedófilo de los mismos, acudiendo inmediatamente a la policía para su denuncia. Este interesante caso ha provocado numerosas dudas que han debido ser resueltas por el Tribunal Constitucional, pues no solo se valorar la casualidad del hallazgo, sino también si hubo o no autorización por el propietario del artefacto informático para acceder a la información. Y de la citada sentencia se puede colegir que no hay vulneración del derecho a la intimidad cuando se verifican las siguientes circunstancias:

1. El titular del aparato lo entrega al técnico para su reparación, poniéndolo a su disposición.

2. El aparato es entregado sin contraseña que evite el acceso por personas ajenas, siendo indiferente -para su análisis constitucional- que esto haya ocurrido por negligencia, descuido o desconocimiento de que en los archivos se contenían vestigios de conductas ilícitas.

3. El descubrimiento de los vestigios del delito tuvo lugar casualmente. Habría que añadir o, mejor dicho, puntualizar que, además de casualmente:

a) El descubrimiento debe ser consecuencia de actos propios de las labores técnicas, efectuadas con la intención de verificar el encargo profesional efectuado por

[5] Sólo a efectos meramente indicativos se pueden ver, entre otras muchas, las sentencias del Tribunal Constitucional 199/2013, de 5 de diciembre; 23/2014, de 13 de febrero; 14/2014, de 30 de enero; 15/2014, de 30 de enero; 43/2014, de 27 de marzo.
[6] STC 173/2011, de 7/11/2011

el propietario del ordenador, y no por mera iniciativa del técnico reparador, con el propósito de penetrar en la vida íntima del cliente. Es decir, que se trata de una conducta que «constituye el protocolo habitual en estos casos».

b) Lo anterior ocurre cuando el técnico ciñe sus actuaciones a la carpeta denominada *mis documentos*; pero otra cosa podría llegar a pensarse si se interviniera en otras carpetas más ocultas o expresamente denominadas de modo que permitieran presumir que tienen un mayor índice de protección y reserva.

El aspecto del consentimiento es, entiendo, bien relevante. Observemos que en el caso expuesto se trata de un aparato que no se encuentra protegido con ninguna contraseña, que no tiene una carpeta protegida especialmente o con una denominación que invite a pensar que su acceso debe ser restringido. Por tanto, el Tribunal Constitucional parece estar diciéndonos que cuando se dan estas circunstancias, si el propietario nos hace entrega del ordenador, está autorizando el acceso a todo aquello que no haya sido protegido con una clave o, al menos, con una denominación protectora. Por consiguiente, si se sigue esa línea, para traspasar esas líneas (la clave o contraseña, la carpeta "privada", etc.) será precisa la autorización judicial emitida conforme al criterio de proporcionalidad antes expuesto.

Esto es coherente con la idea sostenida por el Tribunal Constitucional y por el Tribunal Supremo de que la determinación del ámbito de la intimidad de cada persona compete a ésta. Si uno mismo no acota adecuadamente lo que queda dentro de dicho ámbito, no podrá exigir a los demás que lo respeten.

Tesis esta que permitirá ser utilizada para determinar qué puede y qué no puede ser accedido libremente de los datos que fluyen en el "ciberespacio" o que, más precisamente, se encuentran alojados en algún servidor, físicamente alejado del titular de la información.

Para concluir, conviene destacar que en el ordenamiento español no ha habido una adecuada regulación sobre las medidas de investigación tecnológicas durante muchos años, que ha obligado a los tribunales a hacer una importante e interesante aportación jurisprudencial, por los dos altos tribunales (Tribunal Constitucional y Tribunal Supremo). Por más que esa doctrina no siempre haya sido coincidente, que haya sido criticada y revisada, constituye una aportación importante a la defensa de las garantías de los ciudadanos en esta materia. Actualmente, gran parte de esa producción ha trascendido a la última reforma de la vetusta Ley de Enjuiciamiento Criminal[7], que está ya siendo estudiada y criticada por la doctrina. Ambas fuentes, la jurisprudencia de las últimas décadas y la reforma legislativa, merecen ser estudiadas y tenidas en cuenta, pues constituyen un completo cuerpo regulador de esta materia.

No obstante, si siempre se dice que el Derecho va detrás de la sociedad, temo que eso será más palpable en este ámbito en el que las ciencias informáticas "no corren sino vuelan", cual bajel pirata.

[7] Producida por la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.