4. ALGUNAS CUESTIONES RELACIONADAS CON LA INVESTIGACIÓN DE DELITOS CONTRA BIENES PERSONALÍSIMOS COMETIDOS A TRAVÉS DE REDES SOCIALES O SISTEMAS DE MENSAJERÍA INSTANTÁNEA

La expansión creciente de la delincuencia en la red ha determinado la necesidad de articular herramientas específicas que hagan posible investigar los ilícitos que se cometen en el ciberespacio, identificar a las personas responsables de los mismos y obtener evidencias de uno y otro extremo que puedan ser utilizadas como pruebas válidas en el proceso penal. Para ello, en muchas ocasiones, resultará imprescindible seguir el rastro de las comunicaciones electrónicas relacionadas con la actividad ilícita –para averiguar su origen y las circunstancias en que se han producido– o, en su caso, acceder al contenido de las mismas para clarificar y acreditar en debida forma los hechos objeto de investigación.

Con tal fin es posible utilizar distintas técnicas de investigación que varían según el medio o los medios de comunicación utilizados en el *iter criminis;* así, puede ser necesario proceder al registro de sistemas informáticos y/o de los dispositivos utilizados en la acción criminal por el responsable del delito, la víctima o, incluso, por terceros, o también demandar de quienes hayan actuado como intermediarios en el proceso de comunicación la entrega de los datos almacenados que conserven en relación con ello.

El legislador español ha abordado la regulación de toda esta materia en los Capítulos IV a X del Título VIII del Libro II de la Ley de Enjuiciamiento Criminal, en su actual redacción dada por la LO 13/2015 de 5 de octubre, inspirándose en buena medida en la normativa internacional sobre investigación tecnológica y, concretamente, en los arts. 16 a 21 de la Convención de Budapest del CoE, regulación que ha sido objeto de profundo análisis en las Circulares números 1 a 5 del año 2019 de la Fiscalía General del Estado. Por mor de esta reforma contamos actualmente en España con herramientas de investigación perfectamente adaptadas a las necesidades que plantea la obtención de evidencias electrónicas que sirvan efectivamente como medio de prueba válido para el enjuiciamiento y sanción de las acciones ilícitas desarrolladas en un entorno virtual

No obstante, no hemos de olvidar que estas evidencias electrónicas –así como el reflejo de las mismas en soportes tradicionales obtenidos mediante su impresión o reproducción– son fácilmente manipulables, por lo que su utilización a efectos probatorios en el proceso penal ha de llevarse a efecto con suma cautela, como acertada-

mente recuerdan, entre otras, las SSTS 300/2015, de 19 de mayo, y 754/2015, de 27 de noviembre, que advierten del riesgo de modificación o alteración de este tipo de pruebas. En consecuencia, a fin de acreditar la comisión del hecho delictivo e identificar a sus autores, adquiere también una especial trascendencia la integridad y autenticidad de las evidencias que se presenten a dichos efectos o que se obtengan a resultas de la investigación practicada y, por ende, la posibilidad de que las mismas puedan ser corroboradas contrastándolas con otras fuentes de prueba o a través de pericias específicas, posibilidad que se analiza de forma detallada en el Dictamen 1/2016 de la Unidad Especializada contra la Criminalidad Informática del Ministerio Fiscal [12].

En ocasiones no será preciso acudir a estas técnicas probatorias a efectos de constatar la comisión del ilícito y sus autores porque los propios implicados en los hechos, sin perjuicio de minimizar sus consecuencias, reconocen como ciertas las pruebas de cargo aportadas tales como fotografías, capturas de pantallas o transcripción de conversaciones, circunstancia que se produce con especial frecuencia cuando se trata de comportamientos acaecidos entre menores de edad. Cuando no sea así y resulte necesario obtener las evidencias del delito o se discuta la autenticidad o la posible alteración o modificación de las presentadas, habrá de acudirse a las correspondientes medidas de investigación, entre las cuales tiene especial relevancia el análisis del propio dispositivo utilizado en la ejecución del hecho, ya sea entregado voluntariamente por el investigado –o en su caso por sus progenitores si se trata de un menor de edad– o incautado por las fuerzas policiales o por orden judicial. Dicho análisis, cuya realización exige necesariamente autorización del juez de instrucción, en ocasiones se demora excesivamente por insuficiencia de medios personales y materiales en los organismos que tienen encomendada esta labor, lo que provoca como consecuencia perversa retrasos importantes en el curso de la investigación.

No obstante, en determinados supuestos, el dispositivo o dispositivos utilizados no están a disposición de los investigadores o el resultado de su examen o *volcado* resulta insuficiente o incompleto a los efectos de la indagación en curso. En esa circunstancia resulta imprescindible acudir a otros mecanismos de investigación que presentan peculiaridades específicas, según se trate de ilícitos cometidos a través de las redes sociales o de sistemas de mensajería instantánea, como *WhatsApp, Telegram, Line* o *Snapchat* entre otros muchos.

---

[12] Dictamen 1/2016 sobre la valoración de las evidencias en soporte papel o en soporte electrónico aportadas al proceso penal como medio de prueba de comunicaciones electrónicas.

En el primer caso, resulta determinante que toda la información y contenidos que los usuarios incorporan a esas grandes plataformas de comunicación personal multilateral queden almacenados en las bases de datos de la propia red social durante periodos prolongados de tiempo. Quiere decirse con ello que, con independencia de que el responsable de la actividad criminal utilice una identidad falsa al crear su perfil, borre o modifique la información incriminatoria o, incluso, haga desaparecer íntegramente el perfil mismo para intentar eludir su responsabilidad, toda la información generada al darse de alta en la red (datos de abonado), la relativa a las circunstancia de utilización de la plataforma (datos de tráfico) o a las informaciones publicitadas o comentarios efectuados (datos de contenido) es susceptible de ser recuperada con fines de investigación criminal previa solicitud a los gestores de la red social de que se trate. De hecho, en ocasiones, suele resultar imprescindible solicitar de estos intermediarios la información básica para averiguar el origen de una comunicación y, por ende, iniciar las investigaciones por hechos de esta naturaleza.

Esta aparente ventaja, sin embargo, se ve muy limitada por la circunstancia de que los proveedores de servicio que gestionan las redes sociales tengan generalmente su sede fuera de nuestras fronteras y, con frecuencia, más allá de la Unión Europea, lo que hace que la mayoría de estas solicitudes sean de carácter transnacional, con la complicación que de ello deriva no solo por las diferencias entre los distintos ordenamientos jurídicos sino también por los inevitables retrasos en la tramitación procesal de la causa.

En cualquier caso y para asegurar la conservación de la información que sea de interés –tanto datos de abonado como de tráfico y contenido– es aconsejable solicitarlo así del proveedor del servicio correspondiente, tal y como previene el art. 588 octies LECrim, precepto que se inspira, a su vez, en los arts. 16 y 29 del Convenio de Budapest del CoE. Dicha solicitud, que no precisa autorización judicial, suele cursarse por la Policía Judicial directamente a través de la red 24/7 a la que se refiere el art. 35 del mismo convenio, y generalmente es atendida por los proveedores radicados en países firmantes del mismo, que proceden a conservar la información durante un determinado periodo de tiempo para hacer posible su ulterior remisión al solicitante.

Ahora bien, la petición de entrega de dicha información –a excepción de los datos de abonado que pueden reclamarse directamente por la Fiscalía o la Policía Judicial– exige necesariamente de autorización judicial de conformidad con lo establecido en el art. 588 ter j) LECrim, resolución en la que deberá valorarse la concurrencia de los principios

reseñados en el 588 bis a 1.º del mismo texto legal y, en especial, la proporcionalidad entre la entidad y gravedad del delito investigado y la intensidad de la injerencia en el derecho fundamental. Es por ello, como recuerdan muchos de los fiscales delegados que, en la investigación de un número significativo de los delitos que nos ocupan, particularmente de amenazas y coacciones, la obtención de dicha información puede presentar dificultades si se considera que el hecho ilícito carece de entidad suficiente para justificar medidas de esta naturaleza.

Autorizada judicialmente la solicitud de entrega de los datos, su resultado dependerá de la valoración que sobre la procedencia y oportunidad de dicha petición realicen no solo quienes tengan a su disposición dicha información sino también y, específicamente, los órganos jurisdiccionales competentes del país en el que radica el proveedor de servicios afectado. En ello inciden determinadas circunstancias como la vigencia del principio de doble incriminación –de especial relevancia en el marco de la cooperación internacional– que determinan que, en ocasiones, no se logre la obtención de la información como ocurre, por ejemplo, en aquellos supuestos en los que ha de cohonestarse el respeto al honor o a la dignidad de las personas con el ejercicio del derecho a la libertad de expresión.

En la actualidad se están realizando importantes esfuerzos en el ámbito internacional para facilitar, potenciar y agilizar, con fines de investigación criminal, tanto la preservación como la obtención efectiva de los datos almacenados por los proveedores de servicio, entre ellos, los que gestionan las redes sociales. Así, en el marco de la Unión Europea se está preparando el Reglamento *E-evidence* y una Directiva complementaria al mismo para articular la representación en territorio comunitario, a los indicados efectos, de aquellos proveedores que tengan su sede en terceros países. Igualmente, en el seno del Consejo de Europa se trabaja desde hace meses en la elaboración de un Protocolo Adicional a la Convención de Budapest centrado esencialmente en establecer mecanismos para asegurar el cumplimiento efectivo de las solicitudes de preservación y entrega de información cursadas por otros Estados. Es de esperar que la publicación de estos instrumentos contribuya a mejorar la eficacia en la actuación penal frente a las conductas ilícitas que se cometen a través de estas plataformas de comunicación.

En cualquier caso, no ha de olvidarse que la obtención de información de los propios operadores y proveedores de servicio no es el único medio de acreditar una determinada comunicación o la publicación de un contenido. La incorporación de cualquier tipo de dato en una red social tiene por objeto su divulgación más o menos extendida

según la opción de privacidad/publicidad elegida: accesible solo para los amigos; para amigos de amigos, o de acceso abierto a todos los usuarios. En consecuencia, aun cuando el responsable de la acción criminal haga desaparecer la publicación incriminatoria o incluso el propio perfil, también es factible recuperar la información –y así se efectúa en ocasiones– a través de los datos conservados por cualquiera de los usuarios que haya tenido acceso a la misma en la propia plataforma de comunicación, al igual que también es posible la identificación del usuario o titular del perfil por cualquiera de los medios de prueba válidos en derecho.

Cuando el ilícito se haya cometido a través de *WhatsApp* o cualquiera de los sistemas de mensajería instantánea a los que se ha hecho referencia, los problemas que plantea la investigación criminal cuando no se tiene acceso al contenido supuestamente delictivo o cuando se duda de su integridad o autenticidad, son bien diferentes. Tal y como se encuentra articulada esta modalidad de comunicación interpersonal no existe un intermediario o servidor externo que conserve los mensajes enviados y recibidos, sino que los contenidos únicamente se almacenan en los dispositivos desde los que se realiza la comunicación –que puede ser bidireccional o multidireccional– o, en su caso, en la nube, cuando sea posible optar por esa forma de archivo pero en dicho supuesto tal información únicamente será accesible desde el terminal del propio interesado y se conservará exclusivamente por el plazo que este estime oportuno. Los operadores de telefonía solo podrán facilitar, de haberse conservado, datos relativos al tráfico o a la identificación de los usuarios.

Como quiera que frecuentemente los interesados pretenden probar los ilícitos cometidos en los sistemas de mensajería instantánea por exhibición directa del archivo electrónico en el propio dispositivo, o mediante el conocido vulgarmente como *pantallazo* del mismo, a efectos de corroborar los contenidos de interés resulta de especial utilidad el examen de los terminales implicados en la transmisión, tanto del emisor como del receptor. A dicho fin ha de tenerse también en cuenta que en los supuestos en que se trate de una comunicación multilateral, por ejemplo, las efectuadas en los grupos de *WhatsApp*, el archivo objeto de investigación puede ser localizado en el dispositivo de cualquiera de los participantes en el grupo, a fin de realizar las comprobaciones oportunas.

Este contraste de los terminales afectados –al menos el de origen y el de destino– se hace imprescindible cuando se sospecha que los archivos han sido alterados, eliminados e incluso total o parcialmente simulados. En estos casos es conveniente recurrir a las copias de segu-

ridad que, en estos sistemas de mensajería instantánea se efectúan periódicamente –normalmente una vez al día– y de forma automática. Dicha copia de seguridad se conserva en los propios dispositivos y puede ser recuperada por procedimientos técnico-forenses y su obtención y análisis resulta esencial en orden a detectar supuestas alteraciones o modificaciones del material probatorio disponible.

Ciertamente la investigación de las actividades ilícitas *online* presenta dificultades muy específicas derivadas del medio tecnológico de comisión pero, al tiempo, la circunstancia de que el delito se haya planificado y/o ejecutado a través de procesos de comunicación que quedan indefectiblemente registrados en los sistemas informáticos, pone a disposición del investigador un rastro digital extraordinariamente útil para el esclarecimiento del hecho ilícito y la determinación de quienes hayan participado en el mismo. Lograr aprovechar al máximo las posibilidades que brindan las propias tecnologías, respetando plenamente los derechos fundamentales de los investigados, y en particular la intimidad, el secreto de las comunicaciones y la protección de datos de carácter personal, es el gran desafío al que nos enfrenta esta forma de criminalidad y al que el Ministerio Fiscal está intentando responder con plena sujeción a la ley, imparcialidad y unidad de criterio, a partir de una actuación activa y dinámica cada vez más especializada en esta materia.