diariolaley

El ciberacoso en las redes sociales enfocado desde una perspectiva pericial informática

Javier RUBIO ALAMILLO
Ingeniero Superior en Informática, Perito Informático

Diario La Ley, Nº 35305, Sección Ciberderecho, 20 de Noviembre de 2017, **Wolters Kluwer**

ÍNDICE

Jurisprudencia comentada

TS, Sala Segunda, de lo Penal, Sección Pleno, S 324/2017, 8 May. 2017 (Rec. 1775/2016)
TS, Sala Segunda, de lo Penal, S 754/2015, 27 Nov. 2015 (Rec. 10333/2015)
TS, Sala Segunda, de lo Penal, S 300/2015, 19 May. 2015 (Rec. 2387/2014)

Comentarios

Resumen

El acoso a través de Internet en general y, particularmente, utilizando las redes sociales, se ha convertido en un problema muy serio. Este tipo de acoso afecta, fundamentalmente, a menores, aunque también a personas de todo tipo y en cualquier ambiente: en la pareja, en el trabajo, en grupos sociales como la clase de inglés, etc. Cuando se está sufriendo acoso a través de Internet (ciberacoso), es fundamental saber qué pasos hay que dar y, sobre todo, en manos de qué profesionales ponerse. Los imprescindibles son un abogado y un perito informático colegiado. El abogado denunciará el acoso a la Justicia y, el perito informático, transformará las evidencias del acoso en pruebas, al objeto de obtener una sentencia ganadora para el acosado. Por la propia naturaleza de la tecnología, sin una asesoría técnica competente y colegiada, será muy difícil ganar un caso de ciberacoso si las evidencias no han sido correctamente transformadas en pruebas, algo que sólo un perito informático es capaz de realizar con solvencia.

I. Introducción

El ciberacoso está alcanzando, tristemente, altas cotas de popularidad como delito (o conjunto de delitos) cometido a través de las nuevas formas de comunicación (redes sociales, sistemas de mensajería instantánea, etc.). Este tipo de acoso, ejecutado a través de canales informáticos, constituye una nueva forma del tradicional acoso, pero apoyándose en las tecnologías emergentes y, en muchos de estos casos, en el anonimato aparente o efectivo (ya que, como se explicará posteriormente, ambas formas de ciberacoso coexisten y presentan importantes diferencias),

que las mismas proporcionan.

El acoso a través de redes sociales, sistemas de mensajería instantánea y, en definitiva, Internet, presenta diversas modalidades y variantes, cada una de las cuales puede abordarse desde una perspectiva pericial particular, que ayude a los juristas (abogados, fiscales y jueces), a apreciar el delito desde una perspectiva específica, dando entrada en el proceso legal a la prueba informática de cargo, a través de un informe pericial informático elaborado por un perito informático colegiado.

En un delito de ciberacoso, la prueba informática (1) , que no electrónica (2) , es pieza fundamental en el proceso, pudiendo entrar en el mismo, en cada caso particular, en forma de distintas manifestaciones y siempre avalada por un informe pericial informático (al objeto, sobre todo si se trata de conversaciones mantenidas a través de una red social o a través de una aplicación de mensajería instantánea, de cumplir con los requisitos que establece la STS 300/2015 (LA LEY 57273/2015), confirmada por la STS 754/2015 (LA LEY 196139/2015), que ponen de relieve que las conversaciones pueden ser simuladas o falsas y que, por tanto, necesitan ser avaladas por una pericial informática). Las distintas manifestaciones de una prueba informática pasan por un mensaje de correo electrónico, un mensaje SMS, una o varias llamadas telefónicas, una conversación a través de una aplicación de mensajería instantánea como WhatsApp o Telegram, un mensaje privado (conversación) o público (en el *muro* de un usuario) emitido a través de una red social como Facebook o Twitter, etc.

En definitiva, para que la denuncia a un delito de ciberacoso sea admitida a trámite y enjuiciada, deberá aportarse una prueba fehaciente de que se ha cometido. Actualmente, los simples pantallazos de redes sociales ya no están admitidos como pruebas en base a la jurisprudencia del Tribunal Supremo que se acaba de citar y, por otra parte, el art. 199 del Reglamento de la organización y régimen del Notariado (LA LEY 7/1944), impide que un notario levante actas sobre «hechos cuya constancia requieran conocimientos periciales». Es evidente que un notario no podrá certificar la autenticidad de los mensajes de un muro de Facebook o una conversación de WhatsApp, ya que éstos, como recoge la propia jurisprudencia ya mencionada del Tribunal Supremo, pueden ser falsificados y, por tanto, requieren de los conocimientos de un perito informático. Será una pericial informática, por tanto, la única prueba fehaciente que pueda acreditar que alguien está sufriendo acoso a través de Internet y/o las redes sociales.

II. Anonimato aparente

Muchos acosadores piensan que Internet es anónimo. Y, en parte, tienen razón. En principio, cualquier mensaje enviado a través de Internet, bien de correo electrónico, en una red social, a través de Facebook, Twitter, Instagram, etc., queda identificado unívocamente por una dirección IP desde la que se envía. Una dirección IP es un conjunto de cuatro cifras que van desde cero hasta doscientos cincuenta y cinco, lo que hace un total de dos elevado a treinta y dos direcciones IP posibles para todo el mundo, o lo que es lo mismo, 4294967296 de direcciones IP. Con poco más de cuatro mil millones de direcciones IP en todo el mundo (una cifra, a todas luces, insuficiente, de tal forma que ya está en desarrollo el nuevo protocolo IPv6, que sustituirá al actual IPv4), es necesario establecer un mecanismo que permita la utilización de una misma dirección IP por más de un ordenador. Este mecanismo se conoce como NAT y es implementado por muchas compañías de telecomunicaciones para proveer de acceso a varios abonados con la misma dirección IP, especialmente en redes de datos 3G y 4G, siendo que en redes de tipo ADSL o fibra óptica, por regla general, se concede una dirección IP a un único abonado. Pero, igualmente, a nivel interno, una red doméstica también implementa el mecanismo NAT para comunicarse con el enrutador de nivel jerárquico inmediatamente superior, de tal forma que todos los ordenadores de la misma red local casera tienen, de cara a la operadora, la misma dirección IP asignada por aquélla al enrutador de la red, siendo prácticamente imposible determinar, puesto que los enrutadores domésticos son sencillos y no almacenan una gran cantidad de registros, de qué ordenador de la red partió determinado mensaje o información.

Así pues, se llega a la conclusión de que, en la mayoría de los casos, sobre todo en redes ADSL y de fibra óptica, se podrá identificar la red doméstica o empresarial desde la que partió el mensaje, pero no el ordenador concreto que lo envió. Por otra parte y, como ya se ha indicado, en redes de telefonía móvil, al ser la propia operadora la que ejecuta el mecanismo NAT, por parte, no de enrutadores domésticos, sino de enrutadores pertenecientes al proveedor de acceso al servicio, sí será posible identificar el terminal móvil desde el que se envió el mensaje, porque estos enrutadores están conectados a discos duros de gran capacidad, en los que se almacenan los ficheros de *log* generados por dichos enrutadores y, en los que, en último término, se guardan todas las conexiones realizadas por los usuarios, pudiéndose determinar en qué momento una dirección IP fue asignada y desasignada a qué números de

abonados móviles. Es necesario reseñar que las operadoras, deben almacenar, durante al menos un año, los datos de conexión (pero no el contenido, que está protegido por el derecho fundamental al secreto de las comunicaciones), según se recoge en la Ley 25/2007, de 18 de octubre (LA LEY 10470/2007), de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Por tanto, si se trata de una conexión de ADSL o de fibra óptica, la red podrá ser identificada, aunque no el ordenador de la misma desde el que se envió la información, mientras que si es un teléfono móvil o una tableta, sí se podrá identificar al usuario. El problema reside en que está demostrado que la dirección IP puede suplantarse (*IP spoofing*, en inglés), hecho que motivó la STS 987/2012 (LA LEY 195398/2012), en la que sabiamente se argumenta que el hecho de que una dirección IP sea identificable de forma unívoca con un abonado, no implica que dicho abonado enviase la información comprometida o cometiese el delito investigado. Además, a la posible suplantación de la dirección IP, se unen aspectos técnicos como la facilidad de acceder de forma no autorizada (piratear) a una red inalámbrica —WiFi— doméstica o empresarial, lo cual confirma, aún más si cabe, la dificultad de garantizar que el abonado es la persona que ha cometido el delito.

A este problema debe añadírsele una dificultad previa añadida, que consiste en la obtención de la dirección IP desde la que se envía el mensaje (en caso de que el acoso se produzca a través de una red social, o de un proveedor gratuito de servicios de correo electrónico). Para ello, será necesario un mandamiento judicial y la solicitud de la dirección IP a las sedes centrales de las empresas proveedoras de los servicios, que suelen estar situadas en los Estados Unidos de América y, cuyas sedes europeas, suelen estar radicadas en la República de Irlanda, por las ventajas fiscales que dicho país ofrece. Algunas empresas de este tipo, como Google Inc. o Microsoft Corporation, sí tienen sedes en España (en Madrid y Pozuelo de Alarcón, respectivamente), habitualmente pequeñas y dedicadas mayormente a labores comerciales. Estas empresas, en algunas ocasiones, no contestan a los requerimientos judiciales de España o, en general, de la Unión Europea, ya que se hallan bajo jurisdicción de los Estados Unidos de América, lo cual constituye un problema añadido.

III. Anonimato efectivo

En ocasiones, el ciberacosador es un experto y consigue camuflarse en Internet, utilizando herramientas especializadas o, simplemente, enviando los mensajes desde redes instaladas en lugares públicos, como restaurantes, locutorios, cibercafés, etc. Por ejemplo, utilizando algún tipo de red anónima como TOR, que es capaz de camuflar la dirección IP de origen del mensaje con un sistema de arquitectura de *proxys* (intermediarios), se puede enviar un mensaje cuya dirección IP de origen será la de un *proxy* de la red anónima, siendo imposible conocer la dirección de origen real.

Aun utilizando redes instaladas en lugares públicos o redes anónimas, los delincuentes pueden llegar a cometer errores, por ejemplo, en algunos procedimientos en los que ha participado el perito que suscribe, el delincuente se conectaba, en primer lugar y de manera no anónima, a la red social o programa desde el que cometía el delito y, al poco tiempo, se conectaba al mismo programa utilizando TOR, una vez que, por ejemplo, había ganado acceso al mismo utilizando la contraseña de la víctima, que de alguna manera había averiguado (intrusión no autorizada). En este tipo de casos, es necesario tener en cuenta las conexiones inmediatamente anteriores y posteriores desde la cuenta del usuario que comete el delito, obteniendo todas las direcciones IP desde las que se efectuaron dichas conexiones, en una ventana temporal amplia.

Si se presenta un caso de anonimato efectivo, por ejemplo, a través de una red pública, como la instalada en un locutorio, un hotel o un restaurante, será necesario investigar en otros ámbitos, coincidentes con las horas de envío de los mensajes: registros de visitas, facturas, testigos, cámaras de vigilancia, etc. Por el contrario, si el caso de anonimato efectivo se presenta mediante el envío de mensajes a través de una red anónima, la investigación se complica, siendo necesario solicitar judicialmente la dirección IP desde la que se dio de alta la cuenta en la red social y, posteriormente, comprobar si esa dirección IP corresponde a algún abonado; también habrá que determinar el alias de la cuenta de correo electrónico con la que se registró el usuario en la red social y, comprobar, también mediante orden judicial, desde qué dirección IP realizó el registro, para luego determinar si esa dirección IP corresponde a algún abonado, etc. Es necesario, por tanto, como se suele decir coloquialmente, «tirar del hilo» hasta dar con el origen del ciberacoso.

IV. Ciberacoso no anónimo

En otras ocasiones, los acosadores no se esconden. Utilizan sus cuentas públicas en redes sociales, su teléfono móvil con su número real, etc. En estos casos, lo procedente es presentar una denuncia en el juzgado, acompañada de un informe pericial informático que certifique la autenticidad de los mensajes, tal y como advierte la jurisprudencia de la STS 300/2015 (LA LEY 57273/2015) y la STS 754/2015 (LA LEY 196139/2015), en las que se explica que los mensajes intercambiados a través de cualquier red social, son susceptibles de ser manipulados y, por lo tanto, que deben ser autentificados en un peritaje informático. Posteriormente, desde el juzgado, se deberán solicitar mediante mandamiento judicial, los nombres y apellidos de los titulares de las líneas y/o de las direcciones IP de procedencia desde donde se enviaron los mensajes, al objeto de certificar de forma inequívoca la autoría de los mismos.

V. Tipologías de ciberacoso

Existen numerosos tipos de acoso a través de Internet. A continuación, se detallan los más relevantes.

- Bombardeo de llamadas telefónicas
- Ciberacoso sexual
    - Sextorsión
    - Grooming
    - Etc.
- Ciberacoso en el trabajo
    - Mensajes amenazantes de WhatsApp del jefe, incluso acoso sexual por parte del mismo, ridiculizaciones en grupos de WhatsApp del trabajo, etc.
- Mensajes de correo electrónicos anónimos con amenazas o coacciones
- Ciberacoso escolar
    - Ciberacoso a maestros y profesores
    - Acoso a un maestro en un grupo de WhatsApp
    - Padres que acosan a un profesor
    - Ciberacoso a menores o cyberbullying
    - Ridiculizaciones en grupos de WhatsApp
    - Mensajes amenazantes o comentarios ofensivos en Facebook o Instagram
    - Etc.
- Suplantación de identidad en redes sociales como Facebook, Twitter, Instagram, etc.
- Etc.

Todos los tipos indicados, se pueden englobar en delitos contra la libertad, el honor y la intimidad, como son las amenazas, las injurias, las calumnias, la difamación, etc. También, en el delito de suplantación de identidad, si se produce. Sin embargo, existe un nuevo tipo de delito, incluido en la última reforma del Código Penal, denominado coloquialmente de «hostigamiento», «acoso» o, en inglés, «stalking», tipificado en el art. 172 ter (LA LEY 3996/1995), que consiste en acosar a una persona de manera insistente y reiterada, por cualquier medio. Este delito está castigado con una pena de tres meses a dos años de prisión, o una multa de seis a veinticuatro meses. Las redes sociales y, en general, cualquier herramienta que pueda utilizarse a través de Internet, han propiciado la tipificación de este delito. Es relativamente sencillo, para un experto en Internet, hacer la vida imposible a un tercero a través de la red, persiguiéndole de manera anónima y, sobre todo, aprovechando la información que va dejando la víctima a través de las redes sociales, especialmente en forma de ubicación física de las fotografías subidas a Internet, o incluso de sus comentarios en las redes sociales o a través de las aplicaciones.

Sobre este delito, ya ha habido un pronunciamiento del Tribunal Supremo, concretamente en la STS 324/2017 (LA LEY 31504/2017), en la que se especifica que, para que se considere que se está produciendo un delito de «stalking», se necesita, al menos, un periodo de «hostigamiento» no inferior a un mes (pudiendo llegar hasta seis meses), así como un mínimo de diez intrusiones en la vida privada de la víctima.

La modalidad más preocupante del ciberacoso, es el acoso informático a menores, por parte de otros menores o por parte de un adulto. Los peligros a los que un menor se encuentra expuesto en Internet son incuantificables, correspondiéndoles a los padres o, en su defecto, tutores legales, la vigilancia de los movimientos del niño en Internet y en las redes sociales en las que se encuentre dado de alta. A este respecto, la STS 864/2015 (LA LEY 218893/2015), hace prevalecer la obligación de tutela sobre el menor por encima del derecho a la intimidad del mismo, lo cual autorizaría a los padres o tutores, a llevar a cabo medidas de vigilancia sobre las redes sociales y/o aplicaciones de mensajería que utilicen sus hijos o los menores a su cargo, lo que podría incluso permitir que los padres o tutores utilizasen programas de monitorización o, en la jerga, «espías», en los teléfonos móviles de sus hijos o tutorandos, sin temor a estar incumpliendo ninguna ley.

Por otra parte, es importantísimo reseñar que la instalación de este tipo de sistemas en el terminal móvil de otra persona (distinta a un menor y siempre por parte de su padre, madre o tutor), sin su conocimiento, es un delito muy grave que, entre otros, atenta contra varios derechos de esa persona, como el derecho al secreto de las comunicaciones o el derecho a la intimidad, ambos recogidos en el art. 18 de la Constitución (LA LEY 2500/1978), dentro del Capítulo II, sobre derechos fundamentales y libertades, del Título I. Ningún cónyuge o pareja puede instalar u ordenar instalar, bajo ningún concepto, en el teléfono móvil de su pareja, un sistema «espía» de este tipo, que monitorice mensajes de WhatsApp u otras aplicaciones, posicionamiento GPS, llamadas, etc., constituyendo, como ya se ha advertido, un delito muy grave.

En el caso de tratarse del teléfono móvil que un empresario proporciona a un empleado para desempeñar su trabajo, el empleador sí estaría autorizado a instalar este tipo de programas «espías», siempre y cuando en la empresa exista un protocolo de uso razonable de los sistemas informáticos, que recoja que los mismos pueden ser monitorizados, siendo que el empleado conozca y haya firmado dicho protocolo. En caso contrario, es decir, en el de la inexistencia del protocolo, se estaría generando, según la jurisprudencia (STS del 26/9/2007 (LA LEY 146111/2007) y STS del 6/10/2011 (LA LEY 255452/2011)), una «expectativa de privacidad» que invalidaría esta monitorización. Por otra parte, si el protocolo de uso razonable de los sistemas informáticos aparece recogido en el convenio colectivo al que está suscrita la empresa, en lugar de aparecer en un documento formal entregado al trabajador cuando éste se incorpora a la compañía, también avalaría el uso de este tipo de programas «espías» (STC 170/2013 (LA LEY 145700/2013)).

VI. Redes sociales y aplicaciones de mensajería

Las redes sociales, así como las aplicaciones de telefonía móvil, son el medio más utilizado para la comisión de esta tipología de delitos. Existen diversas redes sociales desde las que se cometen delitos de ciberacoso, como Facebook, Twitter, Instagram, Snapchat, etc. Estas redes sociales, si bien comparten el denominador común de ser servicios capaces de conectar familiares y amigos, o incluso desconocidos, para que puedan intercambiar mensajes, información, fotografías, vídeos, etc., presentan ciertas diferencias entre sí.

Por ejemplo, en Snapchat, la información enviada desaparece una vez ha sido visualizada, siendo muy difícil que pueda ser recuperada y, por supuesto, siendo muy costoso el posible intento de recuperación de la misma. En otras redes sociales, como Twitter, se puede realizar, utilizando herramientas al alcance de cualquiera, un análisis forense para determinar la geolocalización del mensaje 8siempre y cuando el usuario la tenga activa), mientras que, en otras redes sociales o aplicaciones de mensajería, se puede determinar la geolocalización desde la que se ha tomado la fotografía publicada o enviada, examinando los metadatos EXIF de la misma (ya existen muchas otras redes sociales que borran deliberadamente esta información cuando se publica o envía una fotografía).

La cuestión es que, toda esta información, que deja un rastro evidente en Internet de la posible víctima, puede ser usada maliciosamente por su posible acosador. Es imprescindible que, cuando se empieza a notar algún tipo de persecución o acoso, se pondere la posibilidad de moderar o suprimir la actividad en las redes sociales y se tenga en cuenta que, el posible acosador, puede estar aprovechándose de la información que se va publicando o enviando a través de las redes sociales o aplicaciones.

Por otra parte, se debe tener en cuenta que, cuando se está sufriendo acoso a través de las redes sociales, es importantísimo ponerse, desde el primer momento, en manos de un profesional cualificado. La información que se publica en redes sociales como Facebook, Twitter, Instagram u otras similares, puede ser eliminada en cualquier momento por el sujeto acosador, probablemente en el preciso instante en que sea consciente de que la otra persona

le ha descubierto y denunciado a las autoridades. Si no se han tomado las precauciones técnicas apropiadas, esta información habrá desaparecido para siempre y, no bastará con pantallazos de la información, que ya están prohibidos por el Tribunal Supremo, en las ya mencionadas STS 300/2015 (LA LEY 57273/2015), STS 754/2015 (LA LEY 196139/2015) y sucesivas. En WhatsApp, por el contrario, los mensajes recibidos se conservan, pero existe el problema, de que se pueden manipular sin dejar rastro, tal y como fue demostrado por este mismo profesional, en un artículo técnico (3) publicado en su página web, con una notable repercusión en los medios más importantes del país, tales como el diario El Mundo (4) , la cadena COPE (5) o el Telediario de Televisión Española (6) , así como en medios internacionales. Este problema, fundamentado en la sencillez con la que se puede manipular una simple base de datos de tipo SQLite (las utilizadas por la práctica totalidad de las aplicaciones de telefonía móvil), aún no ha sido resuelto por WhatsApp, por lo que es necesario tener mucha precaución a la hora de preservar la cadena de custodia de un terminal en el que se almacenan mensajes sensibles de cara a un procedimiento judicial.

Especial atención hay que prestar a WhatsApp Web. WhatsApp Web es una funcionalidad que permite enviar y recibir mensajes a través de WhatsApp, desde la página web de WhatsApp, es decir, utilizando el ordenador, no el teléfono móvil. Para ello, es necesario escanear, utilizando la aplicación WhatsApp del teléfono móvil, un código QR que se muestra en la web de WhatsApp y, automáticamente, los contactos aparecen en la web y se pueden enviar y recibir los mensajes desde allí, de manera simultánea al terminal. Multitud de personas que no tienen su teléfono móvil protegido por un patrón o por una contraseña, son víctimas de suplantación de identidad y otros delitos mediante el uso, por un tercero de su entorno, de este método, puesto que dicha persona puede tomar el móvil sin su permiso, escanear el código QR de la web de WhatsApp y visualizar los mensajes enviados y recibidos en el terminal desde la web, así como también enviar otros mensajes, suplantando la identidad del propietario del terminal y violando sus derechos al secreto de las comunicaciones y a la intimidad.

VII. Adquisición de la evidencia

En primer lugar, para que una evidencia de acoso informático pueda ser utilizada en un procedimiento judicial, esta evidencia debe convertirse en prueba y, para ello, es necesaria una adquisición de la evidencia para que ésta pueda ser transformada en prueba.

Por ejemplo, en caso de que se trate de acoso efectuado a través de redes sociales como Facebook o Twitter, o un foro de Internet, es necesario realizar una captura de la evidencia con alguna herramienta de tipo *notario digital* o *tercero de confianza*, ya que los simples pantallazos, como ya se ha indicado varias veces, están prohibidos por el Tribunal Supremo en la STS 300/2015 (LA LEY 57273/2015), STS 754/2015 (LA LEY 196139/2015) y sucesivas. Un *tercero de confianza* es una herramienta, regulada en la Ley 34/2002, de 11 de julio (LA LEY 1100/2002), de servicios de la sociedad de la información y de comercio electrónico, en trasposición de la Directiva 2000/31/CE, de 8 de junio (LA LEY 7081/2000), del Parlamento Europeo y del Consejo, relativa a determinados aspectos de los servicios de la sociedad de la información y, en particular, del comercio electrónico, que actúa como intermediario en el que todas las partes implicadas en el proceso confían.

La captura de la evidencia debe realizarse con una herramienta externa de *tercero de confianza*, porque este tipo de evidencias son volátiles, es decir, pueden desaparecer de Internet. Si se produce una denuncia y la evidencia no ha sido capturada, muy probablemente será eliminada cuando el denunciado sea consciente de la denuncia y, una vez haya sido eliminada de la red, únicamente y sólo en algunos casos, podrá ser recuperada durante un periodo de tiempo muy corto, de no más de unos días (el tiempo que dure indexada en las cachés de los diversos buscadores, principalmente Google), para finalmente desaparecer para siempre. Aunque esta ventana de recuperación puede llegar a producirse en algunos casos, en la mayoría de los ocasiones la evidencia nunca podrá ser recuperada.

Si ninguna herramienta de *tercero de confianza* soporta la tecnología de la plataforma a través de la cual se está efectuando el ciberacoso, es necesario, junto al perito informático colegiado, acudir a un notario. El perito informático proporcionará instrucciones precisas al notario que, desde un ordenador instalado en su notaría, deberá conectarse a la plataforma de Internet en la que se esté produciendo el acoso, de tal forma que el notario pueda imprimir, siguiendo las instrucciones precisas del perito informático, la web en la que se produce el acoso y los mensajes, junto a elementos que identifiquen de forma unívoca la web, que le serán indicados al notario por el perito informático. Para ejecutar estas acciones será necesario, muy probablemente, que el acosado introduzca, él mismo, su nombre de usuario o correo electrónico y contraseña, en la plataforma en la que se está produciendo el ciberacoso, sin necesidad de revelar la contraseña ni al notario ni al perito informático. Finalmente, tras producirse la

impresión de los mensajes, se deberá cerrar sesión en la plataforma o red social para evitar que el navegador recuerde la contraseña en el ordenador de la notaría.

Si la evidencia del ciberacoso descansa sobre un correo electrónico, no existe una urgencia tan acuciante como en el caso anterior, ya que por regla general, el correo electrónico no será eliminado por el acusado si éste constituye una evidencia, salvo por error. En cualquier caso, siempre es recomendable salvaguardar la evidencia y realizar la captura de la misma cuanto antes, para evitar la fatalidad de su pérdida accidental. En este caso, se deberán analizar, principalmente, las cabeceras del correo electrónico para comprobar su autenticidad, aunque será necesario tener en cuenta el análisis de muchos más aspectos técnicos, tal y como ya se incidió en un artículo doctrinal, dedicado específicamente al análisis forense de correos electrónicos, escrito por este profesional en esta misma publicación (7) .

Si se tratase de mensajes de tipo WhatsApp, Facebook Messenger o de cualquier otra aplicación de mensajería, incluyendo los clásicos mensajes SMS, la mejor opción es realizar una extracción *física* (8) o *lógica* (9) , en función de la necesidad y del consejo del perito informático, utilizando para ello alguna herramienta estándar como Cellebrite UFED Touch u Oxygen, para posteriormente realizar un análisis forense sobre dicha extracción y determinar la veracidad de los mensajes.

Hay que tener en cuenta que, este tipo de mensajes, por su naturaleza son, como ya se ha indicado, susceptibles de ser manipulados. La única excepción que se puede establecer a la posibilidad de manipulación de mensajes de WhatsApp sin dejar rastro, según las investigaciones llevadas a cabo por este profesional, es que el teléfono en el que se almacenen los mensajes sea un iPhone de Apple, con una base de datos no restaurada desde la *nube* o iCloud de Apple y, además, sin que se haya ejecutado sobre el terminal un proceso de *jailbreak* (es decir, que no se haya vulnerado la seguridad del terminal para acceder al teléfono en el modo de usuario con los máximos privilegios o súper-usuario). Si se dan las tres condiciones, sí se podría garantizar la imposibilidad de manipulación de los mensajes de WhatsApp que se hallen en dicho terminal iPhone (en cualquier terminal Android, así como en cualquier iPhone que no cumpla estas condiciones que se acaban de indicar, los mensajes, a día de hoy, se siguen pudiendo manipular sin dejar rastro).

Por último, si el acoso se produce a través de llamadas telefónicas, es necesario que éstas sean grabadas con alguna de las aplicaciones que permiten la grabación de llamadas telefónicas recibidas en cualquier *smartphone* o teléfono inteligente. La jurisprudencia autoriza a que un individuo pueda grabar una llamada telefónica o cualquier tipo de conversación en la que dicha persona esté presente como interlocutor. Posteriormente, un perito informático deberá autentificar, mediante análisis forense del terminal, que dichas grabaciones no han sido manipuladas (cortadas), es decir, que son íntegras, así como a los distintos interlocutores de la conversación.

VIII. Análisis de la evidencia informática

El análisis forense de la evidencia, determinará la autenticidad e integridad de la misma. La aserción de que la prueba es auténtica reflejará que el autor aparente del acoso, transformado en evidencia, es el autor real y, la aserción de que la prueba es íntegra, significará que ésta es completa y no está alterada ni manipulada.

Para analizar la evidencia, deben utilizarse herramientas forenses de mercado. Por ejemplo, en el caso de que la evidencia sea un correo electrónico, será necesario analizar el mismo con arreglo a lo ya propuesto por el perito que suscribe en un artículo técnico escrito en esta misma publicación (10) , analizando las cabeceras, posibles trazas en servidores, etc. En el caso, de que se trate de mensajes de aplicaciones de telefonía móvil, como por ejemplo, WhatsApp, Telegram, etc., o en general, de cualquier evidencia que se hallare en un terminal móvil, será necesario utilizar herramientas forenses como el UFED Physical Analyzer, adjunto como *suite* a la ya mencionada Cellebrite UFED Touch, estándares ambos a nivel internacional y que, en España, usan habitualmente las Fuerzas y Cuerpos de Seguridad del Estado.

Si se tratara, por ejemplo, de mensajes enviados a través de redes sociales, habrá que verificar, fundamentalmente, la autenticidad de los mismos y, por tanto, identificar la cuenta de origen. Es necesario indicar, en este punto, que el hecho de que una cuenta de una red social tenga nombre y apellidos, no implica, bajo ningún concepto, que la persona real que se halla detrás de esa cuenta sea la que indica su identificación, en lo que podría suponer una suplantación de identidad. Por ello, será vital la solicitud judicial de la dirección IP a la empresa proveedora del servicio y la posterior identificación de la misma, cotejándola a través de las compañías proveedoras de acceso a

Internet.

IX. Redacción del informe pericial informático

El último paso para transformar una evidencia informática en una prueba informática, es la redacción de un informe pericial en el que se plasme, de una manera clara y concisa, comprensible por cualquier lego en informática, todo el procedimiento forense (11) de identificación, captura y análisis de la evidencia. Es importante recalcar una vez más que el procedimiento explicado debe ser *forense,* es decir, repetible por cualquier otro profesional, partiendo de las mismas premisas y llegando a exactamente las mismas conclusiones.

Una vez la evidencia ha sido identificada, capturada y analizada, si se trata de un comentario en una red social, o de un correo electrónico, es muy posible que sea necesario que el juez instructor envíe un oficio al proveedor de servicios de la plataforma, primero, para identificar la dirección IP y, después, a todas las compañías proveedoras de servicios de Internet que operan en España, o incluso la Unión Europea, al objeto de identificar al titular de dicha dirección IP. Esta eventualidad deberá ser explicada y desmenuzada por el perito informático en su análisis forense, para que el juzgador tenga claro lo que debe hacer.

Asimismo, es necesario recalcar, una vez más, que deben tenerse en cuenta todas las aseveraciones que se han realizado, en este mismo artículo, sobre la posibilidad que las empresas proveedoras de los servicios a través de los cuales se han cometido los delitos de acoso (normalmente, redes sociales), no contesten al mandamiento judicial enviado desde España, así como las disquisiciones realizadas sobre el anonimato aparente y el anonimato efectivo del presunto acosador, de tal forma que puede no ser posible la identificación de la dirección IP del acosador o que, aun pudiendo ser identificada dicha dirección IP, no sea posible condenar al presunto culpable del acoso si únicamente se dispone de esa prueba, tal y como ya establece la jurisprudencia.

X. Presentación del informe y ratificación en sede judicial

Como culminación de todo el proceso, el perito informático deberá presentar, siguiendo los cauces adecuados (normalmente, mediante el procurador del procedimiento), el informe pericial en la causa judicial. Por último, deberá ratificarlo en sede judicial cuando le sea notificado por conducto oficial.

XI. Conclusiones

Se puede concluir, para finalizar, por tanto, que es prácticamente imposible que una prueba de carácter informático, en un caso de acoso, sea admitida en un procedimiento judicial si dicha prueba no está avalada mediante una pericial informática firmada por un ingeniero informático colegiado. La STS 300/2015 (LA LEY 57273/2015) y la STS 754/2015 (LA LEY 196139/2015), dejan muy claro que, las pruebas informáticas, especialmente las conversaciones mantenidas a través de aplicaciones de Internet y, generalizando, cualesquiera pruebas de carácter digital, son susceptibles de ser manipuladas, razón por la cual es imprescindible certificar su autenticidad e integridad mediante informe pericial informático.

Si, además, el acoso se produce a través de foros de Internet, correo electrónico o cuentas anónimas en redes sociales, aun pudiendo certificar elementos como la dirección IP de origen desde la que se ha cometido el acoso (que no siempre es posible), será muy difícil encontrar un culpable, tal y como se ha venido señalando a lo largo del presente artículo (es decir, teniendo en cuenta la jurisprudencia del Tribunal Supremo en relación a las direcciones IP).

(1) TARUFFO, Michele, *La prueba*, Ed. Marcial Pons 2008, pág. 85.

(2) RUBIO ALAMILLO, Javier, «La Informática en la Ley de Enjuiciamiento Criminal», *Diario LA LEY,* núm. 8662, pág. 11.

(3) RUBIO ALAMILLO, Javier, http://peritoinformaticocolegiado.es/vulnerabilidad-en-whatsapp-falsificacion-de-mensajes-manipulando-la-base-de-datos/

(4) http://www.elmundo.es/tecnologia/2015/10/01/560d531a22601d40448b459b.html

(5) http://www.cope.es/player/ponedores-whatsapp-rastro-Javier-Rubio-121015&id=2015101205040001&activo=10

(6) http://www.rtve.es/alacarta/videos/telediario/telediario-21-horas-13-10-15/3322221/

(7) RUBIO ALAMILLO, Javier, «El correo electrónico como prueba en procedimientos judiciales», *LA LEY*, núm. 8808.

(8) La extracción *física* de una evidencia móvil es la que se produce *bit a bit*, es decir, elemento mínimo a elemento mínimo, siendo la más completa.

(9) La extracción *lógica* de una evidencia móvil es la que únicamente recoge los datos, accesibles al usuario, de las aplicaciones.

(10) RUBIO ALAMILLO, Javier, «El correo electrónico como prueba en procedimientos judiciales», *LA LEY*, núm. 8808.

(11) Del latín *forensis,* relativo al *Foro.* En la Antigua Roma, los asuntos públicos y que afectaban al pueblo y al mismo Estado, se debatían en el *Foro.* Por tanto, *forense* significa *público.* Un procedimiento *forense* es un procedimiento *público,* es decir, *repetible,* de tal forma que, tras practicar un análisis a una evidencia, con los mismos condicionantes, deben obtenerse siempre los mismos resultados y conclusiones.