PRÁCTICA FORENSE

El correo electrónico como prueba en procedimientos judiciales

Javier RUBIO ALAMILLO

Ingeniero en Informática, Vocal de las Juntas de Gobierno del Colegio Profesional de Ingenieros en Informática de la CAM

Resumen

El correo electrónico se ha convertido en una herramienta clave y de uso universal. Existen numerosos conflictos judiciales en los que una de las partes aporta como prueba uno o varios correos electrónicos, sin que el juzgador, el fiscal y los letrados sean capaces de dilucidar, en la mayoría de las ocasiones, si dichos correos electrónicos son los originales o copias, verificadas o no, de éstos, ni tampoco si han sido técnicamente autentificados y, por tanto, si se trata de pruebas auténticas e íntegras. Asimismo, el auge de las plataformas gratuitas de correo electrónico y su utilización masiva en el ámbito privado, plantea cuestiones importantes relacionadas con la autenticidad de los correos electrónicos intercambiados a través de éstas y que son presentados en causas judiciales. La jurisprudencia relativa a la aceptación del correo electrónico como prueba es, también, variada, con diversas sentencias dictadas por los más altos tribunales, tanto españoles, como europeos, en lo que respecta, sobre todo, al ámbito empresarial.

I. INTRODUCCIÓN

En los tiempos actuales, el correo electrónico es la principal herramienta de comunicación en la empresa. El correo electrónico, actualmente, se ha convertido en el nuevo fax, muy utilizado en las empresas allá por los años 1970, 1980 y 1990, habiendo quedado ya relegado dicho aparato a

mera reliquia en la oficina e, incluso, en la administración pública, tan resistente siempre a los cambios tecnológicos.

A nivel personal, familiar y en las relaciones con otras personas de nuestro entorno cercano (no profesional), el correo electrónico jugó un importante papel en la década pasada, sustituyendo a los medios de comunicación tradicionales como la carta y la postal, pero debido a la intensa vorágine con la que avanza la Informática, ya ha sido relegado a un segundo plano por las redes sociales y las aplicaciones de chat de los teléfonos inteligentes, con las que uno puede comunicarse de forma instantánea con familiares y amigos, sin necesidad de esperar a que la otra persona lea el correo electrónico y conteste el mensaje. A nivel personal, por tanto, es factible decir que el correo electrónico ha muerto, sin embargo, a nivel profesional, se puede considerar que está muy vivo, ya que conserva la formalidad de la carta manuscrita y del fax, no es tan intrusivo en la vida personal del individuo como una aplicación de mensajería instantánea y, aunque no es un medio síncrono, sí es relativamente rápido consultar y contestar los mensajes.

II. DIFERENCIAS ENTRE UN CORREO ELECTRÓNICO ORIGINAL, UNA COPIA VERIFICADA Y UNA COPIA NO VERIFICADA

Debido al uso universal del correo electrónico a nivel, sobre todo, profesional y, también, aunque como decimos, cada vez menos, personal, existen innumerables conflictos en los que interviene el correo electrónico y en los que se aportan mensajes de correo electrónico como prueba en un procedimiento judicial. La admisión o aceptación del correo electrónico como medio probatorio, está supeditada, como toda prueba, a la sana crítica del juzgador. Normalmente, si la parte que aporta la prueba lo realiza en soporte papel y la contraparte no realiza alegaciones sobre la integridad o autenticidad de la prueba, ésta es aceptada sin más. Sin embargo, si la contraparte alega que la prueba no es íntegra o, incluso, que es falsa, la parte que aporta la prueba deberá practicar una prueba pericial que garantice tanto la integridad como la autenticidad de ésta, a fin de poder introducirla en el proceso.

Si la parte que aporta la prueba es requerida para practicar una pericial sobre la misma, la forma de presentar uno o varios correos electrónicos en un procedimiento judicial, mediante informe pericial, debe ser siempre en soporte informático, ya que tanto el perito de la otra parte como el perito judicial, deben tener acceso al dictamen pericial del perito de la parte que aporta la prueba y, a la prueba misma o a una copia forense de ésta. Es, por tanto, absolutamente imposible determinar que un correo electrónico aportado exclusivamente en papel en un procedimiento, aún mediante informe pericial, es auténtico e íntegro, aunque para facilitar el trabajo del juzgador, además de presentar el correo electrónico en soporte informático, se puede aportar también en formato papel mediante impresión.

Desde un punto de vista técnico, aportar un correo electrónico recibido original es impracticable

Un importante dilema que siempre planea sobre muchos profesionales jurídicos, tanto letrados, como fiscales o jueces, en este tipo de procedimientos en los que se aportan correos electrónicos, es si los mismos, aportados en soporte informático (evidentemente, se descartan los aportados únicamente en soporte papel), son originales o no. La respuesta, para la inmensa mayoría de los casos, es que no. Y esta consideración es extraordinariamente importante en el ámbito penal, donde las pruebas constituyen piezas de convicción. Realizando una metáfora con el tradicional

documento en papel, se podría decir que, en la mayoría de las ocasiones, aunque el correo electrónico sea, en origen, auténtico e íntegro, se aporta una fotocopia del mismo, cuando la Ley es clara al respecto y exige, para la presentación de un documento privado, como es un correo electrónico, la entrega del original o, si no es posible, de una copia autenticada por el fedatario público competente (art. 268 de la Ley de Enjuiciamiento Civil).

Aportar un correo electrónico recibido original, es algo prácticamente impracticable desde el punto de vista técnico. Para ello, sería necesario adjuntar al procedimiento el disco duro del servidor al que llegó el correo electrónico, con su correspondiente código hash calculado ante fedatario público, suponiendo que la configuración del servidor conserve los correos electrónicos en el mismo una vez éstos han sido entregados a su destinatario. Salvo que se trate del ámbito penal, en un procedimiento en el que los ordenadores hayan sido intervenidos e incautados por las Fuerzas y Cuerpos de Seguridad del Estado recibiendo órdenes de un juez, no será posible realizar esta aportación, ya que ninguna empresa va a detener su servidor de correo electrónico motu proprio para aportar su disco duro a una causa, menos aún si se trata de una empresa de alojamiento web que preste servicios a varios clientes.

Por otra parte, para que un correo electrónico recibido, adjunto a un procedimiento judicial, fuese metafóricamente una fotocopia compulsada, tendría que aportarse una copia forense del disco duro del servidor de correo electrónico en el que se recibió el mismo antes de ser entregado a su destinatario. En la mayoría de los casos, debido a las configuraciones estándar de los clientes y servidores de correo electrónico, estos últimos siempre eliminan los correos electrónicos cuando los entregan, por lo que, casi nunca, se tendrá la posibilidad de aportar, a un procedimiento judicial, una metafórica fotocopia compulsada de un correo electrónico recibido. En la mayoría de las configuraciones estándar de clientes y servidores de correo electrónico, éstos entregan los correos electrónicos a los clientes, dejando en el servidor unas trazas o apuntes del origen y el destinatario, así como de los instantes de recepción y entrega, pero no almacenan el contenido del mensaje una vez éste ha sido entregado al cliente o destinatario.

Además de esta práctica imposibilidad debido a la configuración estándar de la mayoría de clientes y servidores de correo electrónico, cabe reseñar la dificultad logística que tendría la aportación de una copia forense del disco duro del servidor en caso de permanecer allí el correo electrónico, ya que sería necesario detener el servidor, clonar el disco duro ante fedatario público siguiendo los cauces procesales adecuados y, ulteriormente al análisis de la copia forense del disco, practicado por un perito informático colegiado para determinar la autenticidad e integridad del correo electrónico, aportar finalmente la citada copia forense del disco duro al procedimiento. Si se cumplen todos los cauces procesales adecuados, es decir, si la clonación del disco duro se realiza ante fedatario público (notario o Letrado de la Administración de Justicia), se obtiene el código hash de cada una de las dos copias clónicas del disco original, se levanta acta con los valores de dichos códigos y se realiza depósito notarial o judicial de una de las copias, se puede considerar, a todos los efectos, que la copia forense es idéntica a la original y, por tanto, equivalente a ésta. Se podría, por tanto, hablar en este caso y en términos metafóricos, de que podría aportarse una fotocopia compulsada del correo electrónico a la causa.

Debido, como ya se ha indicado, a que la mayoría de los clientes y servidores de correo electrónico no están

Si es un correo electrónico recibido, es posible aportar una "fotocopia" compulsada

apropiadamente configurados para una eventualidad en la que deban aportarse, a un procedimiento judicial, uno o varios correos electrónicos recibidos, el perito informático únicamente podrá analizar el correo electrónico entregado en el cliente que, evidentemente, no es el original, sino una fotocopia no compulsada —suponiendo que el correo no esté firmado digitalmente— de éste. Puede que, incluso, con un poco de suerte, el perito pueda también analizar las trazas que dejaron tanto la recepción del correo electrónico en el servidor, como su entrega al cliente o destinatario. Así pues, a la causa judicial, en la mayoría de los casos en que se trate de correos electrónicos recibidos, únicamente se podrá aportar lo que metafóricamente sería una fotocopia compulsada de una fotocopia no compulsada de un correo electrónico, con todas las reservas que deben aplicarse sobre una prueba de semejantes características.

Caso aparte es cuando se trata de un correo electrónico enviado en lugar de recibido. En estos casos sí es realmente posible aportar una metafórica fotocopia compulsada, siempre y cuando, evidentemente, se sigan los cauces procesales adecuados y ya explicados de clonación ante fedatario público del disco duro en el que se encuentre dicho correo electrónico, para posteriormente aportar dicha copia clónica al proceso (una copia forense de un disco duro, clonada ante fedatario público, es idéntica a la original bit a bit —es decir, unidad mínima a unidad mínima —, por lo que se puede considerar, a todos los efectos y como ya se ha indicado, la original). Los correos electrónicos enviados permanecen en la bandeja de correos enviados de la cuenta de correo electrónico desde la que se envían, aunque es necesario indicar que, si se desea certificar la recepción de un correo electrónico en destino, no podría garantizarse si éste realmente fue entregado a partir de, únicamente, un análisis del correo electrónico enviado, por lo que sería necesario efectuar también sendos análisis forenses de los servidores de salida y, si es posible, de destino, a fin de corroborar si el correo electrónico realmente llegó.

III. ANÁLISIS FORENSE DE CORREOS ELECTRÓNICOS

Los correos electrónicos no pueden aportarse en un procedimiento judicial sin más, sino

que es necesario llevar a cabo un análisis forense sobre éstos, que ponga de manifiesto la identidad del emisor, la del destinatario, las direcciones IP de origen y de destino, el conjunto de servidores por los que ha pasado el correo electrónico hasta ser entregado, etc.

En el análisis forense de correos electrónicos, las cabeceras juegan un papel fundamental. En terminología de correos electrónicos, una cabecera es un bloque de información, cuyo estándar internacional se especifica en la RFC 822 (actualizada por la RFC 2822) y en la RFC 5322, en las que aparece toda la información relativa al correo electrónico que es necesaria para certificar su autenticidad. Cuando se afronta el análisis de una cabecera de correo electrónico, es muy útil usar un validador de cabeceras, de los que en Internet se pueden encontrar varios. Un validador de cabeceras es, en terminología de gramáticas formales, lo que se conoce como un analizador léxico y sintáctico, que valida que todos los caracteres y cadenas de ídem que aparecen en una cabecera de correo electrónico, son consistentes con el estándar (léxico) y aparecen en las posiciones permitidas (sintáctico), sin entrar a valorar su significado.

Si la cabecera es aceptada por el validador, el análisis de la cabecera ha de efectuarse, generalmente, desde abajo hacia arriba, ya que los distintos servidores por los que pasa un correo electrónico van añadiendo datos al mismo, que se adicionan al comienzo del bloque de

información, por lo que el último servidor por el que pasa el correo electrónico en su camino, siempre aparece en primer lugar, mientras que el servidor de origen, aparece al final.

El correo electrónico deberá ser analizado por un perito informático colegiado

Aun pudiéndose autentificar las cabeceras y certificar que son consistentes, siempre se podría, dando una vuelta de tuerca, alegar que el correo electrónico recibido fue falsificado o alterado en destino, o que se produjo una suplantación de identidad en origen (spoofing). Para descartar absolutamente todas las suspicacias, es necesario que el correo electrónico haya sido firmado digitalmente (no se puede obviar que un correo electrónico sin firmar, no es más que un bloque de texto enviado por Internet, cuya alteración o, incluso, falsificación, incluso sin dejar rastro, tanto si ha sido supuestamente enviado como supuestamente recibido, no presenta demasiadas dificultades). Existen numerosas tecnologías de firma electrónica que permiten que un correo electrónico se envíe firmado (por ejemplo, certificados de la FNMT, que pueden utilizarse en el envío de cualquier correo electrónico, tecnologías como S/MIME, utilizada por Microsoft, DKIM, utilizada por Google y Yahoo, o también OpenPGP, que además permite cifrar los mensajes, utilizada por Edward Snowden para comunicar sus revelaciones sobre el espionaje global de la NSA y la CIA a los periódicos The Washington Post y The Guardian).

Si el correo electrónico no fue firmado digitalmente, nunca se tendría la plena certeza para dictaminar que éste es auténtico e íntegro, pero esta circunstancia tampoco significa que, por sistema, un correo electrónico presentado en un procedimiento, deba ser rechazado al no ser posible determinar su autenticidad e integridad con una certeza absoluta. El correo electrónico deberá, por tanto, ser analizado por un perito informático colegiado, que determinará con un grado de certeza la autenticidad e integridad del mismo. Especial atención deberá prestar el perito al análisis de la cabecera del correo electrónico, con importante énfasis en las direcciones IP de los servidores origen y destino del mensaje, así como en los servidores intermedios por los que pase éste y sus respectivas direcciones IP. Las horas de envío y recepción del mensaje serán también un conjunto importante de datos que deberán ser cuidadosamente analizados por el perito, teniendo siempre en cuenta el posible sesgo de reloj entre la hora de los distintos servidores, así como el contenido del mensaje propiamente dicho. Para finalizar, el análisis de los metadatos o propiedades internas del archivo en el que se almacene el correo electrónico, será también determinante.

IV. SERVICIOS GRATUITOS DE CORREO ELECTRÓNICO

La dimensión del correo electrónico también alcanza a los servicios de correo electrónico gratuito que ofrecen innumerables multinacionales. Las más conocidas a nivel internacional son Google (ahora Alphabet Inc.), con mil millones de usuarios activos a febrero de 2016 en su servicio de correo electrónico GMail, Microsoft con su servicio Outlook.com (del que dependen ya todos los servicios de correo electrónico gratuito que ha ofrecido la compañía a lo largo de su Historia, como MSN, Live o Hotmail), así como Yahoo con su servicio Yahoo Mail, entre otros centenares de proveedores de correo electrónico gratuitos repartidos por el globo (como AOL Mail, propiedad de AOL -Estados Unidos-, Yandex Mail, propiedad de Yandex -Rusia-, o Baidu Mail, propiedad de Baidu -China-, citando algunos de los más importantes).

Este tipo de servicios de correo electrónico juega un papel fundamental en el usuario doméstico, de tal forma que la mayoría de las personas que utilizan diariamente Internet para comunicarse y consumir servicios, tengan o no una cuenta de correo electrónico corporativa que usan,

normalmente y de forma exclusiva, para trabajar, también poseen una cuenta en alguno de estos proveedores, que utilizan constantemente para darse de alta en plataformas web, gestionar los servicios que demandan, comunicarse con familiares y amigos, etc.

El uso de estos servicios de correo electrónico también se refleja en los procesos judiciales. La forma de aportar este tipo de correos electrónicos no debe ser únicamente mediante impresión de los mismos, sino utilizando herramientas de tercero de confianza que certifiquen el contenido de los correos electrónicos, incluyendo las cabeceras de éstos, aportados en un CD o DVD adjunto al informe pericial, en el que sí pueden incluirse impresiones de los correos electrónicos para facilitar la tarea del juzgador, pero indicando que las copias certificadas de los mismos se hallan en el CD o DVD adjunto.

En este sentido, cabe destacar la STS 2047/2015, en la que se establece que cualquier forma de comunicación a través de Internet debe presentarse, en un proceso judicial, avalada por un informe pericial informático, de tal forma que, la presentación de los «pantallazos» de dicha forma de comunicación, son insuficientes para que ésta sea aceptada como prueba. Parece obvio suponer que, si el informe pericial informático se circunscribe exclusivamente a la mera presentación de los «pantallazos» de un correo electrónico, también será rechazado, por lo que será necesario realizar un análisis forense para justificar la autenticidad e integridad de un correo electrónico enviado o recibido a través de un sistema de correo electrónico gratuito.

A este respecto, las herramientas de tercero de confianza proporcionan, como su propio nombre indica, la confianza de que el contenido es auténtico, siempre y cuando el análisis forense que acompañe a las certificaciones realizadas con la mencionada herramienta sea consistente. Por otra parte, en el caso de tratarse de correos electrónicos enviados y/o recibidos en cuentas de correo electrónico pertenecientes a servicios de ídem gratuitos, el juez siempre podrá ordenar que se solicite a los proveedores de dichos servicios y, de forma ulterior a la presentación de las pruebas y su análisis en un peritaje informático, la confirmación de la autenticidad de los mencionados correos electrónicos, aportando las cabeceras de los mismos a los proveedores.

V. JURISPRUDENCIA ESPAÑOLA Y EUROPEA

En España y Europa, las más altas instancias judiciales se han pronunciado dictando sentencias, especialmente enmarcadas dentro del ámbito mercantil, aunque también penal, con respecto a la aceptación del correo electrónico como prueba en los procedimientos judiciales. Asimismo, los Altos Tribunales también han delimitado, en diversas sentencias, el alcance que deben tener las medidas que pueden adoptar los empresarios en relación al correo electrónico corporativo de los empleados.

Así, el Tribunal Constitucional se pronunció, el 7 de octubre de 2013, en su Sentencia 170/2013, avalando que, como el correo electrónico que la empresa pone a disposición de los trabajadores para ejercer su trabajo, es propiedad de la propia empresa, ésta puede monitorizarlo o revisarlo siempre y cuando haya avisado con antelación a los trabajadores y les haya explicado la normativa existente sobre el uso del mismo, o bien, siempre y cuando estas reglas estén recogidas en el convenio colectivo al que estén adscritos la empresa y los trabajadores. Se entiende que, si no se produce tal aviso ni las reglas de uso del correo electrónico están recogidas en el convenio colectivo, el trabajador va a generar sobre el uso del correo electrónico corporativo una «expectativa de privacidad», confidencialidad o intimidad, que determina la ilicitud de la intromisión empresarial en sus comunicaciones.

Esta sentencia se enmarca en la senda que ya estableció el Tribunal Supremo en las Sentencias de 26 de septiembre de 2007 y de 6 de octubre de 2011, en las que determinó que la empresa, como

propietaria de los medios de producción y, también, de los sistemas informáticos que ésta pone a disposición de los empleados para que éstos puedan desarrollar su trabajo, es la que debe determinar las reglas y prohibiciones, totales o parciales, que deben regir sobre el uso de los sistemas informáticos dentro del ámbito privado de los empleados. Así, si la empresa no ha establecido unas normas de uso, no se considera lícito que pueda entrometerse en esta parcela del ámbito del trabajador, en el que se puede haber generado la ya mencionada «expectativa de privacidad» debido a la ausencia de estas normas o reglas que rijan el uso de los sistemas informáticos empresariales.

La diferencia existente entre estas dos Sentencias del Tribunal Supremo y la Sentencia del Tribunal Constitucional es que, en ésta, se considera que el trabajador está avisado sobre la normativa de uso con respecto a los sistemas informáticos que la empresa pone a su disposición, si estas reglas están recogidas en el convenio colectivo al que están adscritos la empresa y los trabajadores.

Posteriormente, el Tribunal Supremo, en su Sentencia 528/2014, explicitó la necesidad de autorización judicial para la intervención de las comunicaciones empresariales a un trabajador en la jurisdicción penal. Sin embargo, la Sentencia establece que, dicha autorización judicial, queda circunscrita expresamente al secreto de las comunicaciones, derecho fundamental recogido en el art. 18.3 de la Constitución y quedando, por tanto, exentos, los datos de tráfico, el historial de navegación, los mensajes que, una vez abiertos por su destinatario, no forman ya parte de la comunicación propiamente dicha, etc., que sí pueden ser presentados sin autorización judicial. Este tipo de información queda excluida del secreto de las comunicaciones debido precisamente al hecho de que la propiedad y tutela de los medios informáticos puestos a disposición del trabajador, recae en la empresa, por lo que esta Sentencia del Tribunal Supremo, está alineada con la Sentencia del Tribunal Constitucional de 7 de octubre de 2013.

Más recientemente, el 12 de enero de 2016, el Tribunal Europeo de Derechos Humanos se pronunció al respecto de una denuncia interpuesta por unos trabajadores de una empresa en Rumanía. En este caso, la empresa accedió a los mensajes de los empleados, tanto profesionales como privados, los leyó e incluso transcribió, de tal suerte que el Alto Tribunal consideró que no existió vulneración de los derechos fundamentales, basándose para emitir tal sentencia en que los mensajes fueron enviados en horario de trabajo y utilizando las herramientas informáticas que la empresa puso a disposición de los empleados.

VI. CONCLUSIONES

La alteración de un correo electrónico, enviado o recibido, no es una tarea difícil. Baste pensar que, un correo electrónico, es un bloque de texto que, si es enviado sin firma digital, puede ser modificado sin dejar rastro sin excesivas dificultades. De la misma forma, tampoco es extremadamente complejo falsificar un correo electrónico desde cero, simulando que fue enviado desde, o recibido en una cuenta de correo electrónico determinada.

Cosa distinta y sensiblemente más compleja, es la suplantación de identidad para enviar, en nombre de un tercero y sin su permiso, un correo electrónico que parezca realmente enviado por dicho tercero. Este tipo de delitos de suplantación de identidad se denominan, tal y como ya se ha mencionado, spoofing, siempre y cuando la dirección de correo electrónico del remitente sea realmente la suya y ésta haya sido suplantada.

Normalmente, este tipo de delitos siempre se acompañan de otros como el phishing, también dentro de la tipología de los delitos informáticos de suplantación de identidad, consistente en obtener información sensible de la víctima a través, habitualmente, de formularios web que

simulan ser los de un tercero en el que el usuario confía, como por ejemplo su entidad bancaria.

Debido a la facilidad, puesta de manifiesto en este artículo, con la que se puede alterar o falsificar un correo electrónico o, sencillamente, incumplir los protocolos procesales que garanticen la cadena de custodia, integridad e inmutabilidad de la prueba a lo largo del proceso, el perito informático, en este tipo de procedimientos, juega un papel fundamental. En todo caso, siempre será esencial cerciorarse de la cualificación del mismo, exigiéndole su carnet profesional de colegiado (y no de asociado o similar, para evitar la contratación de un intruso no cualificado, ya que la mayoría de los intrusos operan bajo la forma de asociaciones), al objeto de certificar su condición de Ingeniero y/o Ingeniero Técnico en Informática, para posteriormente conocer su formación y experiencia en informática forense y judicial, así como sus conocimientos sobre aplicación de protocolos procesales y de conservación de la cadena de custodia de la prueba en el ámbito informático.