

El acuse de recibo (o no repudio en destino)

Josep Lluís Ferrer Gomila
Dpto. de Ciencias Matemáticas e Informática
Apol·lònia Martínez Nadal
Departamento de Derecho Privado
UNIVERSIDAD DE LAS ISLAS BALEARES

El servicio de seguridad denominado «no repudio en destino» fue reconocido como tal por parte de la ISO ya en el año 1989. Pero no ha sido hasta estos últimos años, con la explosión del comercio electrónico y el desarrollo de la Administración digital, que se ha puesto de manifiesto su necesidad real. A pesar de contar con múltiples soluciones técnicas, y de disponer de un marco jurídico en relación al tema del acuse de recibo, todavía queda un último paso: la conjunción de los dos campos. El correo de Internet actual proporciona servicios que reciben el nombre de acuse de recibo, pero que no cumplen los requisitos de seguridad necesarios (son meramente informativos).

El acuse de recibo (o no repudio en destino)

INTRODUCCIÓN

El comercio electrónico y la Administración digital han puesto de manifiesto la necesidad del servicio de acuse de recibo. Este servicio, denominado en el ámbito técnico no repudio en destino, fue reconocido hace ya tiempo por parte de la ISO [1] y de la ITU. Pero las soluciones técnicas por sí solas no son suficientes para dar confianza a los usuarios. También es preciso un marco jurídico que permita conseguir los niveles adecuados de seguridad jurídica y técnica.

Ejemplos de la necesidad del servicio los encontramos en múltiples escenarios: relaciones entre empresarios, empresarios y consumidores, entre administraciones, administraciones y administrados, etc. Un primer ejemplo concreto es el registro de entrada digital, que deberá emitir un acuse de recibo que permita verificar a posteriori que efectivamente un documento se presentó en una fecha determinada y con un contenido concreto. Otro ejemplo son las notificaciones que envía la Administración, para las que hay que garantizar que el destinatario emitirá un acuse de recibo una vez se ponga el mensaje a su disposición. En otro ámbito, el consumidor o el empresario que envían una aceptación contractual a otro empresario, necesitan un acuse de recibo para poder probar que se ha celebrado un contrato electrónico. Un último ejemplo podría ser el acuse de recibo que desea recibir quien realiza un pago electrónico para las posibles reclamaciones.

Como hemos señalado, la existencia de una adecuada cobertura jurídica es esencial para generar confianza. Pues bien, en los últimos años se detecta una actividad notable en la regulación de múltiples aspectos de las nuevas tecnologías en general, y, por lo que ahora nos interesa, del problema del no repudio en destino en particular. Se recogen en este apartado algunas de estas regulaciones, sin ánimo de ser exhaustivos, pues pueden encontrarse muchas otras disposiciones relativas a notificaciones electrónicas, registros telemáticos, etc., pero sí con la intención de exponer las más relevantes o significativas.

Así, en primer lugar, y en el ámbito comercial, ha de mencionarse la recientemente aprobada Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, que, en el Título IV dedicado a la Contratación por vía electrónica, y en concreto el artículo 27.1 (Información posterior a la celebración del contrato), establece que «El oferente está obligado a confirmar la recepción de la aceptación al que la hizo por alguno de los siguientes medios: el envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente, a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la acepta-

ción, ...». Además el punto 2 del mismo artículo indica que «Se entenderá que se ha recibido la aceptación y su confirmación cuando las partes a que se dirijan puedan tener constancia de ello. En el caso de que la recepción de la aceptación se confirme mediante acuse de recibo, se presumirá que su destinatario puede tener la referida constancia, desde que aquél haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones».

Por lo que se refiere a las relaciones con la Administración Pública, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en el artículo 45.5 (Incorporación de medios técnicos) dispone que «Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por éstas u otras Leyes». Por tanto, se admiten los documentos electrónicos siempre que, entre otros requisitos, quede resuelto, en su caso, el problema del repudio en destino.

Este problema es especialmente relevante para la práctica de notificaciones, para las que, de forma general, el artículo 59.1 (Práctica de la notificación) de la misma Ley 30/1992 establece que «Las notificaciones se practicarán por cualquier medio que permita tener constancia de la recepción por el interesado o su representante, así como de la fecha, la identidad y el contenido del acto notificado». Por tanto, aunque no se mencionan expresamente, serían admisibles las notificaciones electrónicas siempre y cuando se pudiera tener constancia de la recepción por el interesado, es decir, en la medida que se resolviera el problema del eventual repudio en destino. Como veremos posteriormente, teniendo en cuenta la trascendencia y problemática de las notificaciones electrónicas, la Ley 24/2001, de 27 de diciembre, introduce un nuevo apartado 3 en el artículo 59 de la Ley 30/1992, dedicado precisamente a esta modalidad de notificación.

Por tanto, a la vista de lo expuesto, existen distintas disposiciones jurídicas que ponen de manifiesto la necesidad de resolver el problema del acuse de recibo. E incluso alguna de ellas trata de resolver, desde el punto de vista jurídico, tal problema. A continuación se exponen y analizan de forma crítica estas posibles soluciones jurídicas y las soluciones técnicas existentes, valorando previamente un servicio ya disponible como es el acuse de recibo del correo electrónico de Internet.

EL CORREO DE INTERNET: VALORACIÓN CRÍTICA

Una primera opción en la que podría pensarse es acudir a servicios que ya se encuentran en funcionamiento para proporcionar el pretendido acuse de recibo. Nos referimos al acuse de recibo del correo electrónico de Internet. Por ello pensamos que debe aclararse su validez. De entrada hay que señalar que el correo electrónico de Internet proporciona dos tipos de servicios de no repudio en destino: lo que denominamos acuse de depósito y un acuse de lectura.

Al primer servicio lo hemos denominado acuse de depósito, porque de hecho puede servir para tener constancia de si un mensaje de correo electrónico ha sido depositado en el buzón del destinatario, o si por el contrario no ha sido posible. Para que sea posible utilizar el acuse de depósito (DSN por Delivery Status Notification), el servidor de correo del destinatario debe ser un servidor «con extensiones», que siga el estándar RFC-1891, SMTP Service Extensions for Delivery Status Notifications.

Pues bien, la respuesta automática que envía el Agente de Transferencia de Mensajes (ATM) que deposita el mensaje en el buzón del destinatario, tiene un formato que se explica en la RFC-1894, An Extensible Message Format for Delivery Status Notifications. Es un mensaje «multiparte» (el contenido es multipart y el subtipo es report) que en concreto contienen tres partes diferenciadas. La primera es una explicación que debe poder leer una persona, y la última, si procede, es el mensaje original o una parte del mismo. La segunda parte es un submensaje del tipo delivery-status (definido en la RFC-1894), cuyo campo más importante es la acción realizada por el ATM informante (failed, delayed, delivered, etc.).

El segundo servicio que puede ser utilizado es el que hemos denominado acuse de lectura, porque puede servir para tener constancia de si un mensaje de correo electrónico ha sido leído por parte del destinatario. Se corresponde con la opción MDN (por Message Disposition Notification) de la mayoría de programas de correo electrónico.

El mensaje que llega al buzón del destinatario será visto por éste como un correo ordinario. Pero hay un campo de cabecera que indica que debe solicitarse al usuario un acuse de lectura. De hecho, inmediatamente que se descargue el mensaje del buzón del servidor, el agente de usuario del destinatario presentará una ventana indicando que se ha solicitado un acuse de lectura (al cual podrá negarse el usuario receptor).

Si el destinatario reconoce (de forma voluntaria) haber recibido el mensaje, el remitente recibirá un mensaje de acuse de lectura. Se trata de un mensaje MIME, y la RFC-2298 (An Extensible Message Format for Message Disposition Notifications) explica el formato de este tipo de mensajes, recogiendo las posibles respuestas. Es un mensaje «multiparte» (el contenido es multipart y el subtipo es report, siendo el tipo de informe disposition-notification) que en concreto contienen tres partes diferenciadas. La primera es una explicación que debe poder leer una persona, y la última, si procede, es el mensaje original o una parte del mismo. La segunda parte es un submensaje del tipo disposition-notification (definido en la RFC-2298), cuyo campo más importante es la acción realizada por el agente de usuario informante en nombre del destinatario del correo. Este campo contiene distintas informaciones. Empieza con el modo de acción (manual o automática), seguido del modo de envío (manualmente o automáticamente), a continuación el tipo de disposición (displayed, dispatched, processed, deleted, denied o failed), y, opcionalmente, los modificadores de la disposición (error, warning, superseded, expired o mailbox-terminated).

La seguridad del servicio que hemos denominado acuse de depósito depende de la confianza que se deposite en el último agente de transferencia de mensajes. Éste puede depositar el mensaje en el buzón del destinatario y no enviar el correspondiente informe al remitente. Y también puede hacer lo contrario: no depositar el correo en el buzón y enviar un informe al remitente notificando el depósito con éxito. La RFC-1894 ya advierte sobre estas y otras posibles falsificaciones.

Podrá pensarse que esto no es fácil o que sucederá muy extrañamente, pero si dejamos la posibilidad abierta, los usuarios podrían escoger proveedores de correo que les permita hacer «trampas». Incluso no sería extraño que algunos usuarios utilizaran su propio servidor de correo electrónico (pensando en la posibilidad de deshabilitar la remisión de acuses de depósito). Desde este punto de vista parece un buen criterio el seguido, como veremos posteriormente, por el Ministerio de Economía consistente en exigir que la dirección de correo que deben utilizar los administrados no puede ser cualquiera, sino que debe ser una dirección proporcionada o validada por el Ministerio. De esta manera, y presuponiendo la correcta actuación de la Administración, se evita el posible fraude, y la Administración tiene más garantías de si se ha depositado un mensaje en el buzón del destinatario o no.

Por otra parte, de la explicación realizada se ha visto que el acuse de depósito que genera el ATM no contiene ninguna información confidencial, ni ninguna firma electrónica. Con ello queremos decir que es un mensaje fácilmente falsificable por parte del remitente, es decir, que un remitente puede construirse un acuse de depósito para el mensaje que desee sin haber transmitido este mensaje. En el caso de la Administración Pública se alegrará que ésta no tiene ningún interés en inventarse un acuse de depósito falso. Pero imaginemos el caso de un funcionario que ha cometido un error, no enviando una notificación en la fecha que debía, y a posteriori intenta cubrir su error con un falso acuse de depósito. La posibilidad, aunque quiera considerarse remota, existe.

Pues bien, un usuario, amparándose en la posibilidad descrita en el párrafo anterior, siempre podrá negar haber recibido un mensaje, y el mecanismo de prueba del remitente (al carecer de ninguna firma, ni del destinatario, ni tan siquiera del agente de transferencia de mensajes) debe ser considerado muy débil.

La RFC-1894 realiza una advertencia, y que de hecho suele explicitarse en los DSNs que se reciben en el correo electrónico de Internet, y es que este acuse de depósito no significa que el destinatario haya leído el correo electrónico. Puede que incluso no sepa que ha recibido este correo. En la remisión de ese acuse de depósito él no interviene de ninguna manera (es su servidor de correo el que se encarga de remitirlo). Por tanto consideramos que no puede darse por recibido un correo en base a estos acuses de depósito. De hecho pueden darse situaciones, que aun cuando extrañas no significa que no se den, en las que el usuario acceda a su buzón de correo, descargue los mensajes allí depositados (por tanto el servidor ya los puede eliminar), y una vez que los mensajes ya están en el ordenador pero antes de que tenga tiempo de leerlos se estropea. En este momento el usuario ha quedado sin la posibilidad de leer esos correos, y sin saber además ni que existen algunos concretos que provocarán que se den por realizadas notificaciones electrónicas. Con todo lo anterior no parece del todo correcto el criterio que, como veremos con posterioridad, establece la normativa administrativa de que una vez depositado un mensaje en un buzón de correo del destinatario y transcurridos diez días, se da por realizada la notificación.

Por lo que se refiere al acuse de lectura, lo primero que hay que decir es que se trata de un servicio que queda a la discreción del destinatario. Si éste lo desea dará la orden de que se envíe, y no lo hará en caso contrario. Por tanto, el hecho de que el remitente no reciba un acuse de lectura como el descrito no significa que el destinatario no haya recibido el mensaje.

Tal como hemos descrito en el acuse de depósito, el acuse de lectura es falsificable (no contiene la firma digital del destinatario, ni ninguna otro parámetro de seguridad). Otra vez, el remitente puede «fabricarse» los acuses de lectura que desee, sin que pueda distinguirse si son reales o falsificados. Siendo así, y amparándose en este hecho, el destinatario incluso podrá rechazar los acuses de lectura que efectivamente él haya enviado. La RFC-2298, relativa a los MDNs, ya advierte en su apartado 6 sobre la posibilidad de que los MDNs sean falsificados tan fácilmente como cualquier correo electrónico ordinario de Internet.

Finalmente, y para ambos tipos de notificaciones, debe tenerse presente que el acuse que recibe el remitente (y en esto se parece bastante al mundo basado en papel) no permite probar que es lo que se recibió, es decir, que el contenido que supuestamente ha tenido a su disposición el destinatario será de difícil prueba.

SOLUCIONES NORMATIVAS

Como es sabido, en los últimos años se ha desarrollado una actividad normativa notable en materia de aplicación de las nuevas tecnologías en la Administración, siendo de destacar especialmente las actuaciones del Ministerio de Economía, y también de la Agencia Española de Administración Tributaria en pos de la Administración digital. Como se ha señalado en la introducción, entre esa normativa administrativa se encuentran distintas disposiciones relacionadas con el acuse de recibo. De entre ellas vamos a analizar la Orden de 26 de diciembre de 2001, que aborda jurídicamente la problemática de las notificaciones electrónicas, aun cuando sólo es aplicable de forma sectorial en el ámbito del Ministerio de Economía, y el nuevo artículo 59.3 de la Ley 30/1992, que regula de forma general las notificaciones electrónicas, pues es aplicable de forma general en la Administración.

En primer lugar analizamos la Orden de 26 de diciembre de 2001 por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos por el Ministerio de Economía y los Organismos Públicos adscritos al Departamento y se crea un Registro Telemático para la presentación de escritos y solicitudes. En concreto, nos detenemos en el punto 6 del apartado 4 (Condiciones generales para la presentación de escritos, solicitudes y comunicaciones): «En el caso de que, de acuerdo con el ordenamiento aplicable, se admita la notificación telemática utilizando buzones de correo electrónico, en el sitio web del Ministerio de Economía se mantendrá actualizada una lista de proveedores que ofrezcan servicios de correo electrónico con las especificaciones que previamente se establezcan».

A falta del desarrollo de las citadas especificaciones, a priori parece que desde el Ministerio de Economía se ha detectado el problema del acuse de recibo. Como ya se ha indicado, si permitimos que las notificaciones se envíen a una dirección electrónica arbitraria, ésta puede corresponder a un proveedor de servicios de Internet en connivencia con el destinatario de la notificación o ser el propio destinatario quien mantenga su propio servidor de correo. En estos casos, el servidor de correo podrá entregar el correo al destinatario de la notificación, y por otra parte remitir un acuse de recibo «negativo» indicando que ha sido imposible entregar la notificación en el buzón del destinatario (alegando distintos posibles motivos: buzón no operativo, servidor en recuperación, etc.). En cualquier caso recordemos que siempre podría ser rechazado a posteriori, pues los acuses de lectura y de depósito no llevan asociada ninguna firma digital del emisor de esos acuses de lectura o depósito.

La misma Orden en su Anexo III establece los criterios específicos de utilización de técnicas telemáticas correspondientes a cada uno de los procedimientos administrativos. Por lo que respecta a la presentación telemática de recursos y reclamaciones se establecen los siguientes pasos:

- Acceder con el navegador al pertinente formulario en www.mineco.es/recursos.
- Cumplimentar los datos solicitados en el anterior formulario.
- Anexar los ficheros oportunos con un segundo formulario.
- Enviar el formulario cumplimentado y los ficheros, pulsando el botón FIRMAR Y ENVIAR.
- Si el recurso o reclamación es aceptada, el sistema devolverá en pantalla los datos del documento presentado, mediante un preimpreso normalizado, indicando la persona que presenta el recurso o reclamación, la dirección del correo electrónico para envío de notificaciones al interesado, la fecha de presentación, el número de orden dentro del Registro Telemático que

hace el recurso, la fecha y hora en que queda registrado en el Registro Telemático el recurso y la huella digital generada.

Obsérvese que el acuse de recibo que remite el Ministerio de Economía, sólo es informativo, pues no contiene ninguna firma digital que vincule a la Administración. Esto significa que en caso de disputa a posteriori, sobre si una reclamación fue sometida o no, y si lo fue a su debido tiempo, el administrado no dispondrá de elementos de prueba a su favor. Estas disputas pueden surgir por posibles fallos del sistema, por posibles acciones con mala fe por parte de algún funcionario, y, siendo consciente de las dos posibilidades anteriores, también podría haber mala fe por parte del administrado.

Junto a esta normativa sectorial, es de interés analizar la regulación jurídica de las notificaciones electrónicas en el ámbito de la Administración en general. Como hemos señalado, teniendo en cuenta la importancia de las notificaciones electrónicas para el desarrollo de la Administración digital, la Ley 24/2001, de 27 de diciembre, en el artículo 68.2 modifica la Ley 30/1992, añadiendo, precisamente un nuevo apartado 3 a su artículo 59 dedicado específicamente a esta forma de notificación: «Para que la notificación se practique utilizando medios telemáticos se requerirá que el interesado haya señalado dicho medio como preferente o consentido expresamente su utilización, identificando además la dirección electrónica correspondiente, que deberá cumplir con los requisitos reglamentariamente establecidos. En estos casos, la notificación se entenderá practicada a todos los efectos legales en el momento en que se produzca el acceso a su contenido en la dirección electrónica. Cuando, existiendo constancia de la recepción de la notificación en la dirección electrónica, transcurrieran diez días naturales sin que se acceda a su contenido, se entenderá que la notificación ha sido rechazada con los efectos previstos en el siguiente apartado, salvo que de oficio o a instancia del destinatario se compruebe la imposibilidad técnica o material del acceso». La misma Ley 24/2001 modifica en su artículo 30.3 la Ley General Tributaria 230/1963, de 28 de diciembre, añadiendo un apartado 8 en el artículo 105 de idéntico contenido al nuevo artículo 59.3 de la Ley 30/1992.

La nueva regulación de las notificaciones electrónicas del artículo 59.3 de la Ley 30/1992 para la Administración en general, y del artículo 105.8 de la Ley General Tributaria, para el ámbito tributario en particular, nos sugiere tres comentarios. Por una parte es necesario definir cómo se determinará el momento en que se produce el acceso al contenido de la dirección electrónica. Ya hemos indicado que el mecanismo actual de acuse de lectura del correo electrónico de Internet no nos parece una vía adecuada. Si el sencillo acceso al buzón ya presupone que se ha recibido la notificación, todavía nos parece más grave, pues el acceso al buzón no garantiza la descarga correcta de los correos entrantes que allí se encuentren depositados.

De forma análoga es absolutamente necesario definir cómo se tendrá la constancia de la recepción de la notificación en la dirección electrónica. Ya hemos expuesto con anterioridad que no nos parece correcto utilizar los mecanismos actuales que hemos denominado acuse de depósito. La Administración podría erigirse en tercera parte de confianza, argumentando que cuando afirme que se ha depositado un correo en el buzón del destinatario no admite discusión. Pero hay que resaltar que esto deja al administrado en una clara posición de indefensión, pues le correspondería la carga de proporcionar una prueba diabólica para probar lo contrario. En cualquier caso deben quedar explicitados ambos mecanismos.

Finalmente, parece excesivo que si el usuario no accede a su buzón en el plazo de diez días, se dé por rechazada la notificación. Esto significa que desde el momento que decidimos utilizar las técnicas telemáticas para recibir notificaciones de la Administración, no podemos dejar de consultar el correo electrónico por un plazo superior a nueve días. Además, se perjudica al usuario «electrónico» frente al usuario «papel». A este último, en caso de no recoger los correspondientes avisos que puedan dejarse en el buzón convencional, no se le aplica el rechazo (que tiene la implicación de que el procedimiento sigue

su curso como si se hubiera realizado la notificación, que es lo que indica el artículo 105.5) sino que se procede al intento de notificación por otras vías (publicación en el Boletín Oficial correspondiente). No se entiende muy bien por qué no se procede de la misma manera con los usuarios «electrónicos».

SOLUCIONES TÉCNICAS

El acuse de recibo, o el no repudio en destino, forma parte de una familia de servicios en los que dos o más partes desean intercambiar elementos electrónicos, con la particularidad de que ninguna de las partes quiere entregar su elemento sin tener la garantía de que recibirá el elemento de la otra parte. Este tipo de transacciones reciben el nombre de intercambio equitativo de valores. Ejemplos de estos intercambios son la firma electrónica de contratos (intercambio de copias firmadas del contrato), el correo electrónico certificado (un mensaje por un acuse de recibo) y el pago electrónico a cambio de un recibo.

Los protocolos para el intercambio equitativo de valores deben proporcionar a las partes la suficiente evidencia para poder probar al final del intercambio si éste tuvo lugar y con que contenido. Diremos que un intercambio es equitativo si al final del mismo, o cada parte dispone del elemento que esperaba recibir, o ninguna de las partes tiene información que comprometa a la otra parte [2]. Pues bien, en la bibliografía, e incluso en el mercado, podemos encontrar soluciones particulares para la firma de contratos, el correo certificado y el pago por recibo. Pero carecemos de estándares con efectiva implantación, y tampoco se ha realizado una validación desde la perspectiva jurídica.

Un primer tipo de soluciones (para el acuse de recibo) se basa en el intercambio gradual de secretos (las partes intercambian las evidencias de no repudio de forma simultánea). Esta aproximación [3] consigue la equitatividad a través del intercambio gradual de información en múltiples iteraciones: en cada iteración se revela una pequeña parte de la información que debe ser intercambiada. Desde un punto de vista técnico, esta aproximación es demasiado ineficiente para una implementación real. Además, la equitatividad se basa en la suposición de que las partes disponen de la misma potencia de cálculo. Esta suposición es poco realista en la práctica y desde el punto de vista teórico debe ser descartada. Desde un punto de vista jurídico, este tipo de soluciones no se adaptan a los modelos establecidos (por ejemplo el esquema de la Ley de Comercio Electrónico: oferta - aceptación - acuse de recibo). Por otra parte, sería difícil convencer a un juez sobre si se recibió o no un acuse de recibo utilizando ese método.

Un segundo tipo de soluciones son los protocolos con tercera parte de confianza (las partes intercambian los elementos asistidos por una TTP, Trusted Third Party). Podemos encontrar varios protocolos que utilizan una TTP [2, 4, 5]. Pero los protocolos con TTP difieren en el grado de implicación de la misma. Podemos clasificar este tipo de protocolos en dos clases: con TTP activa (la TTP está activamente implicada en cada ejecución del protocolo) y con TTP subsidiaria o protocolos «optimistas» [6] (la TTP sólo interviene en caso de excepción, y no en todas las ejecuciones del protocolo). Pero las soluciones con TTP también presentan inconvenientes: la tercera parte de confianza puede convertirse en un cuello de botella. Además, las TTPs desearán cobrar por su intervención. Por tanto, desde el punto de vista técnico, y también desde el económico, uno de los objetivos a la hora de diseñar un protocolo eficiente para el intercambio equitativo de valores es reducir al máximo la intervención de la TTP.

Como conclusión, los protocolos «optimistas» son especialmente interesantes. Las partes intercambiarán sus elementos directamente, siguiendo los pasos especificados en el protocolo, confiando recibir los elementos de la otra parte. Así será si el protocolo finaliza con éxito. Si por el contrario, una de las partes intenta hacer trampas (o se producen errores en la comunicación) la otra parte debe poder contactar con la TTP para que solucione la situación no equitativa.

Los requisitos formales para el intercambio equitativo «op-

timista» con TTP fueron formulados en [2], y reformulados en [5]: efectividad, equitatividad, sin dependencias temporales, no repudio y posibilidad de verificar el comportamiento de la tercera parte. Dos propiedades adicionales que se deberían cumplir son la eficiencia y la privacidad (esta última como propiedad opcional según el deseo de los usuarios). Ahora, desde el punto de vista jurídico, debemos añadir un nuevo requisito: que las soluciones técnicas sean conformes al marco jurídico establecido. Por ejemplo, para la firma electrónica de contratos, en el derecho español, es necesario que los protocolos sigan el esquema oferta - aceptación - acuse de recibo.

Finalmente, pensamos que las soluciones deben ser seguras desde el punto de vista técnico, pero tan sencillas como sea posible. Algunas disputas deberán ser resueltas en los tribunales, y los jueces deberán evaluar las pruebas aportadas por las partes implicadas en el intercambio. Obviamente los jueces serán asistidos por peritos, pero al final deberán entender las conclusiones proporcionadas por esos peritos.

CONCLUSIONES

Creemos que es clara la necesidad del acuse de recibo en distintos ámbitos. Por una parte disponemos de soluciones técnicas que proporcionan soluciones válidas al problema, y por otra parte de un marco jurídico que debería ser completado para dar seguridad al tráfico electrónico de datos. En cualquier caso, será necesario un último paso que será la conjunción de los dos campos: validar las soluciones técnicas desde el punto de vista de la reglamentación en vigor. Este hecho, junto con la falta de estándares implantados, hace necesaria una intensa investigación (en la doble vertiente: jurídica y técnica), y la actuación de proveedores de servicios y productos en el ámbito de la seguridad de las comunicaciones.

Finalmente creemos que es necesario eliminar la falsa sensación de seguridad, y no confiar en mecanismos (como los acuses de recibo del correo electrónico de Internet) que no son solución al problema planteado. De lo contrario, corremos el riesgo de arbitrar una Administración digital o un comercio electrónico, que deberá afrontar costosos litigios que dejarán a una de las partes en situación de desventaja (por falta de pruebas fehacientes o admisibles). v

2 Josep Lluís Ferrer Gomila

Profesor Titular de Ingeniería Telemática
Departamento de Ciencias Matemáticas e Informática
Universidad de las Islas Baleares
dijjfg@uib.es

2 Apol·lònia Martínez Nadal

Profesora Titular de Derecho Mercantil
Departamento de Derecho Privado
Universidad de las Islas Baleares
dpramn0@uib.es

BIBLIOGRAFIA

- [1] ISO Technical committee / subcommittee JTC 1: «Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture». ISO 7498-2, 1989.
- [2] N. Asokan, V. Shoup y M. Waidner: "Asynchronous Protocols for Optimistic Fair Exchange". Proceedings of the IEEE Symposium on Research in Security and Privacy, páginas 86-99, Oakland, California, 1998.
- [3] I.B. Damgård: "Practical and provably secure release of a secret and exchange of signatures". Advances in Cryptology - Proceedings of Eurocrypt'93, LNCS 765, Springer Verlag, páginas 200-217, Lofthus, Norway, 1993.
- [4] J.L. Ferrer, M. Payeras y L. Huguet: "Efficient Optimistic N-Party Contract Signing Protocol". Proceedings of 4th Information Security Conference, ISC 2001, LNCS 2200, Springer Verlag, páginas 394-407, Málaga, España, 2001.
- [5] J. Zhou, R. Deng y F. Bao: "Some Remarks on a Fair Exchange Protocol". Proceedings of Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, LNCS 1751, Springer Verlag, páginas 46-57, Melbourne, Victoria, Australia, 2000.
- [6] N. Asokan, M. Schunter y M. Waidner: "Optimistic protocols for fair exchange". Proceedings of 4th ACM Conference on Computer and Communications Security, páginas 7-17, Zurich, Switzerland, 1997.