

INSTRUMENTOS ELECTRÓNICOS DE PAGO

Por
VIRGINIA VEGA CLEMENTE
Doctora en Derecho. Abogada

SUMARIO: RESUMEN. ABSTRACT.- 1. CONSIDERACIONES GENERALES.- 2. INSTRUMENTOS DE PAGO APLICADOS AL COMERCIO ELECTRÓNICO.- 3. INSTRUMENTOS DE PAGO TRADICIONALES ADAPTADOS AL COMERCIO ELECTRÓNICO.- 4. INSTRUMENTOS DE PAGO ESPECIALMENTE DISEÑADOS PARA EL COMERCIO ELECTRÓNICO.- 5. EL DINERO ELECTRÓNICO.- 5.1. Planteamiento general. 5.2. Naturaleza Jurídica.

RESUMEN

El pago es la forma normal de extinguirse las obligaciones. El comercio electrónico basa su peculiaridad en la vía de perfección del contrato, pero ello no es óbice para que el cumplimiento de la obligación por parte del consumidor o usuario revista la forma tradicional de pago: efectivo, tarjeta de crédito, cheque, letra de cambio o cualquier otra forma que pueda utilizarse en el comercio convencional.

Hemos de comprender que este sistema tradicional de cumplimiento no es todo lo efectivo que pueda desearse en el comercio electrónico, de ahí que hayan surgido otras formas o modalidades de cumplimiento para adaptarse a las exigencias del medio contractual.

Una de las cuestiones que más preocupan al consumidor es la del medio de pago, sobre todo en las formas surgidas por mor de las nuevas tecnologías. El éxito del comercio electrónico pasa, pues, por la adopción de medios técnicos y normas jurídicas que tiendan a garantizar la seguridad del tráfico.

Junto al problema de la seguridad está el del anonimato, que es un factor importante en algunos tipos de pago, en concreto en el pago mediante dinero electrónico.

ABSTRACT

The payment is the normal form of extinction of obligations. Electronic commerce based their peculiarity in the way of perfection of the contract, but that do not prevent the fulfilment of the obligation by the consumer or user from taking the traditional form of payment: cash, credit card, check, bill of exchange or any other form that can be used in conventional trade.

We must realize that this traditional system of compliance is not as effective as can be desired in electronic commerce, hence encountered other forms or methods of compliance to adapt to the demands of those contracts.

One of the issues that most concern the consumer is the payment method, especially in emerging forms due to of new technologies. The success of electronic commerce lies, then, in the adoption of technical and legal rules that tend to ensure traffic safety.

Along with the problem of security is that of anonymity, which is an important factor in some types of payments, particularly in payment by electronic money.

1. CONSIDERACIONES GENERALES

El término pago se deriva del latín “pacare”¹, que originalmente se utilizaba para expresar el acuerdo entre dos partes implicadas en un conflicto, mediante la entrega de una unidad de valor aceptada por costumbre o tradición². La evolución en el tiempo de esta unidad de valor, así como los mecanismos de intercambio, ha sido propiciada por la aparición de nuevas actividades en la economía y de innumerables innovaciones técnicas, que día a día transforman rápidamente, no sólo la forma de hacer negocios, sino también nuestra propia forma de vida o trabajo.

Esta materia es otra de las relevantes para el desarrollo y la implantación del comercio electrónico³. Internet se presenta como un nuevo escenario en que los empresarios ofrecen bienes y servicios a los consumidores, dando lugar a contratos que se perfeccionan a distancia⁴ y en los que, también a distancia, puede tener lugar la ejecución del mismo, es decir, el pago⁵.

La idea de pagar por bienes y servicios valiéndose de instrumentos electrónicos no es nueva y, de hecho, si miramos a nuestro alrededor, podemos apreciar pruebas claras de transacciones en que, al menos, parte del proceso se ha llevado a cabo por vía electrónica⁶. Pero la implantación de Internet ha provocado que lo que en su momento fueron frustrados y complicados intentos de implementar sistemas de pago de ordenador a ordenador, sean hoy realidades que permiten completar todo el proceso de pedido, compra, entrega del bien o servicio y pago a través de la red. Y desde este punto de vista, se plantea la cuestión acerca de si es suficiente con

¹ Pacificar o hacer paz.

² En esta línea, ESCUDERO CALLEJA/GONZÁLEZ ÁLVAREZ, “Intermediación de Servicios de Pago”, *Comunicaciones de Telefónica I+D*, número 20, marzo 2002.

³ GONZÁLEZ-CALERO, F. R., *Aspectos Jurídicos del Comercio Electrónico, en especial la Protección de Datos, La Firma Electrónica y la Propiedad Intelectual*, 2ª Edición, Madrid, 2003, pp. 32 y ss.

⁴ La Directiva 97/7/CE, del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia, define el contrato a distancia como aquel que tiene lugar “entre un proveedor que, para dicho contrato, utiliza exclusivamente uno o más técnicas de comunicación a distancia hasta la celebración del contrato, incluida la celebración del propio contrato”.

⁵ Efectivamente se habla de la posibilidad de que el pago tenga lugar a distancia aunque no siempre habrá de ser así, como ocurre en el caso del pago contra reembolso.

⁶ Vid. MATEO HERNÁNDEZ, J. L., *El dinero electrónico en internet. Aspectos técnicos jurídicos* Ed. Comares, Granada, 2005, pp. 55 y ss.

adaptar los sistemas de pago existentes y hasta ahora utilizados en el comercio tradicional para hacerlos entrar en juego como plataformas de pago en Internet, o si se hace imprescindible la elaboración de específicos sistemas de pago cuyo terreno de aplicación sea única y exclusivamente el proporcionado por la red.

La dogmática en general acerca de la materia no varía en absoluto y los principios rectores del pago en general resultan en su totalidad aplicables a la concreta modalidad del pago electrónico⁷.

El pago, que equipara la mayor parte de la doctrina al cumplimiento⁸ de una obligación, vendrá dado por toda transferencia de fondos⁹ realizada por el comprador al vendedor utilizando un instrumento electrónico de pago en cumplimiento de la obligación contraída¹⁰. Un medio de pago¹¹ será “todo aquello que tenga poder liberatorio de las obligaciones”¹², o toda forma de dar cumplimiento a la obligación contraída¹³.

Los instrumentos de pago¹⁴, definidos por BERNAL JURADO como “aque-
llos mecanismos mediante los cuales se inicia la transferencia de los medios de

⁷ Si bien, se dan una serie de peculiaridades en materia de dinero electrónico o en temas relacionados con el uso de tarjetas de débito o crédito.

⁸ DÍEZ PICAZO, L., *Fundamentos del Derecho Civil Patrimonial. Las relaciones obligatorias, Volumen II*, Tecnos, Madrid, cit., pág. 472.

⁹ Como reconoce LARENZ, el deudor no debe cosas, sino un valor económico; deudas que reciben un tratamiento general en el artículo 1.170 del Código civil que dispone que “*el pago de las deudas de dinero deberá hacerse en la especie pactada, y, no siendo posible entregar la especie, en la moneda de plata y oro que tenga curso legal en España*”, que desde el 1 de julio de 2002 es el euro, en virtud del artículo 109 L del Tratado de la Comunidad Europea, y los artículos 3 y 4 de la Ley Orgánica 10/1998, de 17 de diciembre, complementaria de la Ley sobre introducción del euro.

¹⁰ Lo realmente decisivo será apreciar si el pago cumple, y de qué modo, los efectos de todo pago, sin entrar en innecesarias consideraciones sobre la naturaleza jurídica.

¹¹ El medio de pago sobre el que gira todo el entramado de instrumentos de pago, sean tradicionales o electrónicos, es el consistente en entregar una determinada cantidad de dinero. Efectivamente, como apunta DÍEZ PICAZO, “aunque en términos generales, las obligaciones pueden consistir en entregar una cosa o en hacer algo, en una economía medianamente avanzada y fundada en la división del trabajo, el dinero opera como instrumento de intermediación en los cambios y, por consiguiente, como uno de los más importantes objetos de las posibles prestaciones que se insertan en una relación obligatoria”.

¹² Vid. BERNAL JURADO, E., *El mercado español de tarjetas de pago bancarias*, Editorial Civitas, Colección Economía, Madrid, 2001, pág. 48.

¹³ Vid. MATEO HERNÁNDEZ, J. L., *El dinero electrónico en internet, op. cit.*, pág. 59.

¹⁴ Si bien no existe una definición legal de pago electrónico, se considera como tal la realización de pagos a través de medios electrónicos. Por tanto, entrarían dentro de la definición de pago electrónico todos

pago (en esta caso el dinero) entre las partes implicadas en una transacción”¹⁵, serán los mecanismos utilizados a través de Internet para transmitir el medio de pago del deudor al acreedor¹⁶.

El concepto de medios electrónicos de pago lo encontramos en el ámbito europeo en la Recomendación 97/489/CE¹⁷ relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular las relaciones entre emisores y titulares de tales instrumentos, que entiende por tales “...aquellos que permiten efectuar transferencias de fondos, retirar dinero en efectivo y la carga de un instrumento de dinero electrónico en los cajeros automáticos, y el acceso a los fondos de la cuenta en una entidad (instrumentos de pago de acceso a distancia)”.

Al configurar una modalidad de las TEF, el dinero electrónico es regulado en forma general por la normativa que regula las TEF¹⁸. No obstante esta regulación

los pagos efectuados mediante instrumentos electrónicos de pago que se realicen a través del empleo de medios electrónicos. Cabe señalar que tampoco existe una definición legal única sobre qué ha de entenderse por instrumento electrónico de pago. Con carácter general, puede señalarse que estarían dentro de los instrumentos electrónicos de pago aquellos que permiten el acceso a distancia a una cuenta bancaria, considerándose en particular como tales las tarjetas de pago y el dinero electrónico, en cualquiera de las formas en que pueda presentarse el mismo, almacenado bien en una tarjeta inteligente o bien en una memoria de ordenador.

¹⁵ Vid. BERNAL JURADO, E., *El mercado español de tarjetas de pago bancarias*, op. cit., pág. 48. Dicho autor continúa su exposición afirmando que “en el caso de pago con efectivo, ambos conceptos (medios e instrumentos de pago) coinciden por cuanto la entrega de moneda o billete tiene por sí misma poder liberatorio de deudas. Sin embargo, en caso de pago sin efectivo, el medio de pago transmitido es el dinero bancario y los mecanismos utilizados para ello (tarjetas, cheques, transferencias, domiciliaciones, ...) son simples sustitutivos transitorios de aquéllos. Tal es el caso de una transferencia bancaria; en este caso el instrumento utilizado sería la transferencia y el medio de pago el dinero bancario”.

¹⁶ Tratándose de obligaciones pecuniarias por Internet, lógicamente se deben valorar las reglas generales que el Código civil contiene en materia de pago de deudas de dinero, y en este sentido, su artículo 1.170 se limita a declarar que el pago “deberá hacerse en la especie pactada y, no siendo posible entregar la especie, en la moneda de plata u oro que tenga curso legal en España”, añadiendo el artículo 1.445, en sede del contrato de compraventa, que la obligación del comprador no consiste sino en pagar “un precio cierto, en dinero o signo que lo represente”. Por lo tanto, no existe obstáculo alguno que coarte la utilización de otros sistemas de pago distintos de los tradicionales siempre que cumplan con los criterios básicos que rodean todo pago, criterios que como veremos más adelante no encuentran dificultad alguna en su aplicación al terreno de los instrumentos de pago electrónico.

¹⁷ DOCE L 208 de 2 de agosto de 1997.

¹⁸ En Estados Unidos las TEF son reguladas por primera vez en la EFTA, sancionada por el Congreso el 10 de noviembre de 1978 e implementada a través de un reglamento específico denominado “Regulation E” de la *Federal Reserve Board*. La EFTA, promulgada con el objeto de proteger los intereses particulares de los consumidores usuarios de los sistemas de transferencias electrónicas de fondos, se

de carácter general, la preocupación por regular el dinero electrónico propiamente dicho, se ha hecho sentir sobre todo en el ámbito comunitario, donde existen diversos textos legales reguladores¹⁹.

En materia específica de dinero efectivo electrónico, es de destacar la adopción de la Directiva 2000/46/CE del Parlamento Europeo y del Consejo, de 18 de septiembre de 2000, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades, (conocida comúnmente como Directiva sobre entidades de dinero electrónico), como único texto legal sistematizado orientado a regular la emisión del dinero efectivo electrónico. La normativa contenida en la Directiva citada, establece un marco reglamentario orientado hacia el reconocimiento mutuo de la autorización y supervisión cautelar de las entidades emisoras de dinero electrónico que operan

encarga de regular, entre otros aspectos, las relaciones contractuales entre las instituciones de crédito y sus clientes para el servicio de las TEF, las obligaciones del banco frente a sus clientes y los deberes de éstos frente a la institución financiera, de igual manera se establece el régimen de responsabilidad de la institución por el incumplimiento de una orden de TEF. Uno de los aspectos más importantes de la EFTA es la regulación que se establece en materia de tarjetas sobre la responsabilidad del consumidor en el uso de la tarjeta y sobre la prohibición de emisión de tarjetas no solicitadas. Al lado de la regulación de la EFTA, existe la regulación contenida en el artículo 4A del *Uniform Commercial Code* que regula las transferencias de fondos de elevada cuantía que generalmente se compensan y liquidan en las cámaras de compensación bancaria. La diferencia entre ambos cuerpos legales se advierte en un doble aspecto, en primer lugar, la EFTA como ley federal, es aplicable a todos los estados de la Unión mientras que el ámbito de aplicación del artículo 4A se restringe a aquéllos que lo hayan adoptado; de otro lado, la EFTA está encaminada principalmente a proteger los derechos de los consumidores en tanto que el artículo 4A del UCC se dirige a regular las transacciones de mayor cuantía generalmente ejecutadas entre empresas o instituciones financieras. En el Derecho comunitario, las transferencias de fondos en general son reguladas por la Directiva 97/5/CE del Parlamento Europeo y del Consejo de 27 de enero de 1997 relativa a las transferencias transfronterizas, dictada con el objeto de regular las transferencias realizadas por los particulares y las pequeñas y medianas empresas 2 efectuadas en cualquiera de las divisas de los Estados que forman parte de la Unión Europea, traspuesta al ámbito español mediante la Ley 9/1999 de 12 de abril por la que se regula el régimen jurídico de las transferencias entre Estados miembros de la Unión Europea. En el ámbito internacional, la CNUDMI ha elaborado la Ley Modelo sobre Transferencias Internacionales de Crédito con el objetivo de armonizar las prácticas internacionales y lograr una normativa uniforme en la materia. Un estudio de estos textos puede consultarse en PERALES VISCASILLAS, P., "Transferencias bancarias: Directiva 97/5/CE, Ley Modelo de UNCITRAL y Artículo 4A UCC", en *Derecho de los Negocios*, N° 88.

¹⁹ Dentro de estos textos destacan: (1) La Comunicación de la Comisión al Consejo Europeo: Una nueva baza para Europa: las tarjetas de pago electrónicas de 12 de enero de 1987, dirigida principalmente a conseguir la interoperabilidad de las tarjetas electrónicas en los diferentes Estados miembros, (2) la

dentro del territorio comunitario, a través del establecimiento de una licencia única con supervisión en el Estado de origen, de modo que permita aprovechar las ventajas derivadas de la utilización del dinero electrónico y fomentar su uso²⁰.

Con el fin de completar la incorporación al Derecho español de la Directiva 2000/46/CE se ha aprobado el Real Decreto 322/2008, de 29 de febrero, sobre el régimen jurídico de las entidades de dinero electrónico²¹. Este Real Decreto se configura “como una norma de procedimiento”, y se estructura en torno al régimen jurídico de la creación de entidades de dinero electrónico (EDE), el régimen de supervisión prudencial, la limitación de actividades y obligación de realizar determinadas inversiones y el régimen de inversión.

Es imprescindible determinar la importancia que el comercio electrónico en torno a los medios de pago desempeña en la economía comparada con el volumen total de la actividad comercial. Las operaciones realizadas por medios telemáticos y en concreto a través de Internet representan todavía un papel secundario²², si

Recomendación de la Comisión Europea 87/598/CEE de 8 de diciembre de 1987 relativa a un Código de buena conducta en materia de pago electrónico, (3) la Recomendación de la Comisión 88/590/CEE de 17 de noviembre de 1988, relativa a los sistemas de pago y en particular a las relaciones entre titulares y emisores de tarjetas, dirigida a orientar las cláusulas contractuales a elaborar por las entidades emisoras de tarjetas en sus relaciones con sus clientes, (4) la Recomendación de la Comisión 97/489, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de tales instrumentos, (5) la Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social de 1 de julio de 1998, sobre un Marco de actuación para la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, (6) la Resolución del Parlamento Europeo de 13 de enero de 1998 sobre el dinero electrónico y la Unión Económica y Monetaria donde se recomienda a la Comisión a presentar una propuesta relativa a la creación de un marco reglamentario para la emisión de dinero electrónico con el objeto de crear un marco adecuado que permita a las instituciones que cumplan los requisitos de confianza, interoperabilidad y estabilidad en el sistema financiero, y (7) El Informe del Banco Central Europeo sobre el dinero electrónico en el que se analizan los riesgos provenientes del uso de estos nuevos medios de pago, principalmente aquellos derivados de los sistemas basados en tarjetas de prepago o software específicos desarrollados para realizar pagos a través de una red de telecomunicaciones como Internet.

²⁰ Un estudio amplio sobre esta Directiva puede consultarse en ROMERO FERNÁNDEZ, J. A., “El marco jurídico de las entidades de dinero electrónico: perfiles jurídico-privado”, en *RCE*, Nº 17 de 2001.

²¹ Este Real Decreto se dicta en ejercicio de las competencias que atribuye al Estado el artículo 149, 1, 6ª, 11ª y 13ª y en virtud de la habilitación otorgada al Gobierno por el artículo 21 noveno de la Ley 44/2002, de 22 de noviembre de medidas de reforma del sistema financiero, para desarrollar el régimen jurídico aplicable a la creación y condiciones de ejercicio de la actividad de las EDE y, en particular, para el establecimiento de su capital inicial mínimo, exigencias de recursos propios permanentes, régimen de inversiones, así como las limitaciones a sus actividades comerciales.

bien las tasas de crecimiento siguen siendo en la actualidad muy elevadas. Una de las limitaciones que frenan el desarrollo de esta nueva forma de negocio que viene motivada por las reservas y reticencias de que los consumidores han hecho gala, debido fundamentalmente a la falta de posibilidades o acceso, así como la escasa confianza²³. Habrá que tener en cuenta en un futuro los nuevos avances tecnológicos que están siendo fruto de experimentación en la actualidad y que en breve, y una vez resulten adecuadamente implementados, pueden traer consigo un nuevo salto cualitativo en la forma de hacer negocios a través de Internet.

La seguridad resulta necesaria con carácter general para el funcionamiento del comercio electrónico y, en particular, respecto de la utilización de medios de pago electrónico en redes abiertas, como Internet, en las que se plantean una serie de cuestiones con el fin de garantizar la propia realización del pago mediante la utilización de sistemas de pago electrónico que pueden resultar vulnerables ante acciones ilícitas de terceros.

En concreto, la seguridad en la realización de pagos electrónicos viene garantizada actualmente mediante la utilización de protocolos de seguridad como SSL (*Secure Sockets Layer*)²⁴ y SET (*Secure Electronic Transaction*)²⁵. Dichos protocolos no son sino normas técnicas mediante las que se posibilita la transmisión segura de información a través de redes abiertas.

²² Sobre todo si analizamos el comercio electrónico con consumidores o B2C.

²³ Vid. Dictamen del Comité Económico y Social sobre *La Incidencia del comercio electrónico en el mercado interior* (OMU). D. O. C123 de 25.4.2001.

²⁴ Este protocolo fue diseñado en el año de 1994 por Netscape con el objetivo de proteger el acceso de personas no autorizadas a determinada información confidencial. El protocolo SSL proporciona los servicios de cifrado de datos, autenticación de servidores, integridad de mensajes y, en menor grado, la identificación del cliente para conexiones TCP/IP (*Transmission Control Protocol/Internet Protocol*). El protocolo SSL proporciona un canal de comunicaciones entre los servidores y los navegadores a través del cual, cifrando los datos intercambiados, las partes pueden celebrar transacciones electrónicas con seguridad. El SSL funciona de forma sencilla, se basa en la encriptación de los datos mediante la utilización de una clave de sesión y la aplicación de una clave pública (normalmente la RSA). El funcionamiento del protocolo SSL puede resumirse en 4 fases: 1. La denominada "Fase Hola", momento en el cual el navegador y el servidor se deben poner de acuerdo respecto a los algoritmos necesarios para mantener la confidencialidad y la autenticación. 2. Una vez alcanzado el acuerdo se inicia la "Fase de Autenticación", etapa en la cual el servidor envía al navegador el certificado que contiene su clave pública, solicitando al mismo tiempo el certificado del cliente. 3. Después, el cliente envía al servidor una clave maestra, con la cual se genera la clave de sesión que cifrará los datos que las partes intercambien a través del algoritmo de cifrado acordado. La clave de sesión es remitida por el usuario debidamente cifrada gracias a la utilización de la clave pública del servidor. Esta parte del proceso se conoce como "Fase de

Adquiere especial atención la cuestión relativa a la fiscalidad de los medios de pago electrónico, ya que debe recordarse que el Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados (ITPyAJD) grava los documentos notariales, mercantiles y administrativos, teniendo de esta manera incidencia sobre la utilización de instrumentos electrónicos de pago.

Al gravar los documentos mercantiles dicho impuesto, se plantea la cuestión de si las formas de pago que pueden considerarse incluidas dentro de una definición en sentido amplio de dinero electrónico y, en cualquier caso, dentro del concepto de instrumentos electrónicos de pago, quedan o no sujetas al pago del mencionado impuesto.

En este sentido, la jurisprudencia del Tribunal Supremo ha señalado que también se gravan por el ITPyAJD los instrumentos que tengan una función de giro en el tráfico mercantil, independientemente de que los mismos tengan o no la calificación de documentos.

Se trata por tanto de una cuestión que requiere de una respuesta concreta, pudiendo tenerse en consideración la necesidad de no establecer obstáculos que impidan el desarrollo de dichos instrumentos electrónicos de pago, lo que además supondría gravar los mismos con un impuesto que no se aplica al resto de medios de pago que pueden calificarse como tradicionales.

Creación de Clave de Sesión". 4. Por último, en la "Fase de Verificación" se comprueba tanto la autenticidad del servidor y del usuario, como la seguridad del canal establecido. Concluida esta última fase, se da inicio a una sesión segura entre las partes. Si bien es cierto que ofrece un sistema seguro para el envío y cifrado de los números de tarjetas de crédito, también lo es que carece de la capacidad para proteger otros aspectos de la actividad comercial (verificar que la tarjeta sea válida, autorizar la transacción con los bancos, etc.). Otra desventaja es la protección parcial que concede, ya que garantiza la integridad y confidencialidad de los datos únicamente durante el tránsito de los mismos, pero no los protege una vez que los mismos son recibidos por el servidor. A pesar de estas deficiencias, el SSL es un protocolo seguro cuya utilización es altamente recomendable para proteger las transacciones electrónicas. Sin embargo, para lograr una óptima protección, lo mejor es utilizar tanto el protocolo SSL como el protocolo SET, pues así se gozaría al mismo tiempo de la seguridad proporcionada por ambos sistemas.

²⁵ Este protocolo fue diseñado con la intención de asegurar y autenticar la identidad de las personas que participan las transacciones efectuadas a través de cualquier red en línea. Fue desarrollado por iniciativa de Visa y Mastercard, y con la participación de diversas empresas como Microsoft, IBM, Netscape, SAIC, GTE, RSA, VeriSign y otras empresas líderes en tecnología. El objetivo primordial de SET es mantener la confidencialidad de la información intercambiada en una transacción, así como garantizar la integridad del mensaje y la identidad de los participantes, con objeto de evitar los fraudes, falsificaciones y uso ilegítimo de tarjetas de crédito en Internet. El SET proporciona los medios para que consumidores y comerciantes se identifiquen entre ellos antes de la realización de la transacción. Su funcionamiento se

Existe un gran número de instrumentos de pago que permiten el cumplimiento de las obligaciones pecuniarias a través de Internet, aunque de momento sólo unos pocos gozan de una implantación práctica efectiva y sólo unos cuantos elegidos son los que por ahora captan la atención o confianza del consumidor²⁶.

Los sistemas electrónicos de pago pueden clasificarse en múltiples categorías, si atendemos a la magnitud del pago, nos encontramos con dos grandes grupos: los empleados para efectuar macropagos y los utilizados para pagos de escasa cuantía, comúnmente denominados micropagos.²⁷

basa en la utilización de certificados digitales y de la encriptación de claves públicas para proteger la información financiera de los participantes. Es importante recalcar que, para evitar cualquier clase de fraude, el SET está diseñado de tal forma que la empresa, en cuyo favor se realiza la transacción, nunca podrá tener acceso ni conocerá el número de la tarjeta usada por el consumidor. El mecanismo de una transacción realizada utilizando el SET es similar al de las transacciones ordinarias, celebradas utilizando como medio de pago una tarjeta de crédito. Una transacción SET se desarrolla de la siguiente manera: 1. El protocolo SET da inicio en el momento en que el cliente decide adquirir un determinado artículo o servicio. 2. El servidor del comerciante realiza una descripción del pedido, con lo cual pone en marcha la aplicación "cartera del cliente". 3. Se cifra y se transmite la orden de pago. Se incluyen tanto los datos del pedido como las instrucciones de pago. 4. Se envía la petición del pago al banco del comerciante. 5. El banco descifra la información recibida, verifica la identidad del comprador y del comerciante, y comprueba la integridad de los datos. Si todo es correcto, envía una petición de autorización de pago al banco emisor (banco del cliente). 6. El banco del emisor verifica los datos y, si todo es correcto, autoriza la transacción. 7. Después, se envía al comerciante un testigo de transferencia de fondos, el cual comprueba que todo se ha desarrollado correctamente. 8. El software del cliente prepara y envía a éste un recibo de la transacción. A continuación se completa el procesamiento del pedido (envío de mercancías o suministro de servicios). 9. Realizada con éxito la transacción, el comerciante genera una petición de transferencia a su banco solicitando el abono en su cuenta del precio pactado. 10. Se hace el cargo en la cuenta correspondiente a la tarjeta de crédito utilizada. El SET aún no está completamente implantado en Internet debido, en primer lugar, a la necesidad de utilizar un software especial (tanto para compradores como para comerciantes) cuya distribución y comercialización se está desarrollando muy lentamente. La segunda y más importante razón es que el funcionamiento del SET resulta complejo y confuso para los usuarios. Desde el punto de vista de los especialistas, SET es un mecanismo que irá creciendo paulatinamente, pero de momento seguirá coexistiendo con el protocolo SSL.

²⁶ Vid. MATEO HERNÁNDEZ, J. L., *El dinero electrónico en internet*, op. cit., pág. 91.

²⁷ MATEO HERNÁNDEZ, en este caso, distingue entre sistemas de micropagos, pagos de escasa cuantía y pagos de mayor cantidad (*micropayments*, *low-value payments* y *high value payments*): "En virtud de esta clasificación, en el terreno de los micropagos se incluirían específicos sistemas por los que se crea una moneda específica que opera entre comerciante y cliente, de un valor reducido, para hacer frente a compras de muy escasa cuantía. [...] Por lo que respecta a los pagos de escasa cuantía, destacar la aparición del denominado dinero electrónico [...] que se presenta como un sistema de especial relevancia en esta terreno, y que puede utilizarse para realizar pagos en el entorno tradicional y también en Internet. Finalmente, y en relación con las transacciones de mayor cuantía, las tarjetas de pago, en sus diversas

Otra clasificación que resulta de especial utilidad, se refiere a la funcionalidad del método empleado, en este sentido hablamos de sistemas de prepago, postpago y pago simultáneo. Esta diferenciación adquiere importancia práctica y jurídica ya que nos sirve para determinar el momento en que el pago ha tenido lugar y el deudor queda liberado de su obligación. Dentro de los medios de prepago ubicamos el dinero electrónico y algunos sistemas de micropago que exigen el almacenamiento previo del dinero en el soporte respectivo (la tarjeta, el disco duro del ordenador, la cuenta de correo, etc.). En el ámbito de los sistemas de pago simultáneo, las tarjetas de débito, cuyo funcionamiento se basa en una transferencia electrónica de fondos que tiene lugar simultáneamente a la presentación del instrumento. Dentro de los sistemas de postpago, los cheques electrónicos y las tarjetas de crédito, en estos casos, habrá que esperar que el pago se haga efectivo o que el dinero sea ingresado en la cuenta del vendedor para que se produzcan de manera plena los efectos solutorios del pago.

Una tercera clasificación alude al soporte electrónico utilizado para instrumentalizar el medio de pago.

Se hace necesario establecer una clasificación que comprenda los instrumentos de pago tradicionales que, tal y como se vienen utilizando en el comercio tradicional, son también empleados para realizar compras a través de la red de redes; sin olvidar, en segundo lugar, que alguno de esos instrumentos de pago ha sido objeto de especial adaptación para su concreta aplicación a las compras realizadas a través de Internet; para terminar haciendo especial referencia a aquellos instrumentos que han sido específicamente diseñados para ser utilizados en el concreto escenario proporcionado por las autopistas de la información.

2. INSTRUMENTOS DE PAGO APLICADOS AL COMERCIO ELECTRÓNICO

En este grupo se incluyen formas o instrumentos de pago tradicionales como el pago contra-reembolso, la transferencia, el cheque, la domiciliación bancaria o la tarjeta de crédito, utilizados del mismo modo y bajo los mismos presupuestos

modalidades se han erigido como un medio eficaz, relativamente seguro y masivamente aceptado para hacer frente a la obligación contraída, sin olvidar las ya mencionadas transferencias electrónicas de fondos y los avances que se están llevando a cabo en el ámbito de los títulos valores electrónicos, destacando el caso del cheque electrónico". *Vid.* MATEO HERNÁNDEZ, J. L., *El dinero electrónico en internet*, *op. cit.*, pp. 73 y ss.

que en las operaciones comerciales ajenas a la red. Y es que como reconoce MADRID PARRA, “aun cuando un contrato se haya celebrado por medios electrónicos, a la hora de su consumación, el cumplimiento de la obligación del pago se puede llevar a cabo por medios tradicionales o por los más modernos que facilitan las nuevas tecnologías. Teóricamente nada lo impide, pero prácticamente supondrá, en la mayoría de los casos, una distorsión no acompasada con los medios tecnológicos utilizados para la fase de perfección del contrato”²⁸, ya que no podemos negar que el pago realizado en Internet utilizando medios tradicionales convierte al proceso en caro, lento, incómodo e inapropiado.²⁹ Nos referimos a formas de utilización de instrumentos de pago que podemos calificar como primitivas, dentro del actual contexto del comercio electrónico.

3. INSTRUMENTOS DE PAGO TRADICIONALES ADAPTADOS AL COMERCIO ELECTRÓNICO

De acuerdo con el Banco Central Europeo³⁰ pueden apreciarse diversos mecanismos y diferentes técnicas que se han implementado a fin de adaptar formas de pago tradicionales para su idónea utilización en operaciones de comercio electrónico, destacando fundamentalmente el caso de las tarjetas de crédito³¹, las transferencias electrónicas de fondos³² y los instrumentos de débito³³.

²⁸ Vid. MADRID PARRA, A., “Seguridad, pago y entrega en el comercio electrónico”, *Revista de Derecho Mercantil*, núm. 241, julio-septiembre de 2001, Madrid, pág. 1212.

²⁹ En este sentido, *vid.* CARRASCOSA LÓPEZ, V., POZO ARRANZ, M^a. A., RODRÍGUEZ CASTRO, E. P., *La contratación informática: El nuevo horizonte contractual. Los contratos electrónicos e informáticos*, 3^a Edición, Granada, 2000, pág. 37.

³⁰ Vid. *Informe del Banco Central Europeo*, en “E-Payments in Europe. The Eurosystem ‘s Perspectiva”, de 16 de septiembre de 2002, pp. 9 a 16.

³¹ Especiales protocolos diseñados para proporcionar una alta seguridad y una total autenticación de los sujetos intervinientes, comprador y vendedor. Además, y siguiendo con la tendencia dirigida a la consecución de un instrumento de pago seguro y confidencial se ha desarrollado la posibilidad de hacer uso de números de tarjetas de crédito *virtuales*. Es de sobra conocido que la mayor traba a la expansión del comercio electrónico a través de redes abiertas es la sensación de inseguridad que experimentan los consumidores y usuarios a la hora de transmitir datos confidenciales, en especial los números de sus cuentas bancarias o tarjetas de crédito. Técnicas como la firma electrónica suponen un avance en lo relativo a la seguridad *on-line*. No hay que olvidar, empero, que cualquier avance informático en esta materia no debe entenderse al margen de las disposiciones legales vigentes. Lo que es técnicamente seguro no tiene por qué ser jurídicamente seguro, ni lo jurídicamente válido tiene siempre que estar ligado a técnicas de seguridad infalibles. Por poner un ejemplo, el mayor temor de los usuarios de tarjetas es el que algún

4. INSTRUMENTOS DE PAGO ESPECIALMENTE DISEÑADOS PARA EL COMERCIO ELECTRÓNICO

Son sistemas específicamente pensados para operar a través de Internet, de los que destacamos los siguientes:

a) Sistemas de acumulación de pagos. Nos encontramos ante esquemas³⁴ que se utilizan para la realización sucesiva de pequeños pagos que se van acumulando durante un determinado periodo de tiempo para luego ser cargados al comprador como un único pago de mayor cuantía³⁵. Hay que destacar que en la utilización de estos sistemas específicos no se precisa el envío de datos personales o sensibles a través de las redes telemáticas, y pueden ser empleados como instrumentos de pago eficientes para completar micropagos³⁶.

desaprensivo se apodere del número de dichas tarjetas y las use discrecionalmente, lo que, creen, supondría perder el importe de los cargos efectuados a su cuenta. Sin embargo, existen preceptos y principios legislativos que eximirían al titular de la tarjeta de crédito de responder por cualquiera de estos cargos. La única forma de que un tercero realice pagos electrónicos con una tarjeta ajena es prescindiendo de la firma digital, pues ésta le identificaría al instante y dejaría en evidencia que la identidad de la persona que utiliza la tarjeta y el titular de la misma no coinciden. Es por ello que el usurpador deberá realizar los pagos a través de un sistema que no permita su identificación. Y aquí es donde entra en juego la Ley, pues en el artículo 46 de la Ley de Comercio Minorista se establece que cuando el importe de una compra hubiese sido cargado utilizando el número de una tarjeta de crédito, sin que ésta hubiese sido presentada directamente o identificada electrónicamente, su titular podrá exigir la inmediata anulación del cargo. De esta forma se llega a la conclusión de que el uso de tarjetas de crédito en la red no supone un problema al menos para los consumidores y usuarios de la red. Y es que la parte "débil" en las transacciones electrónicas es el comerciante, que es a quien corresponde probar que su abono está justificado (a no ser que responda el Banco o entidad financiera titular de la tarjeta, todo depende del contrato que tenga con el comerciante). Es por ello que se deduce que el avance en las tecnologías de seguridad en la red basadas en el cifrado y la firma digital son necesarias para el establecimiento de un comercio electrónico seguro, sin perjuicio de que, hasta que su implantación se generalice, los mayores perjudicados de la falta de seguridad en las redes, en cierto modo, no serán los consumidores y usuarios sino las empresas que ofrecen sus productos a través de la Red.

³² También se está potenciando la utilización de esta concreta forma de pago en las compras *on line* de bienes y servicios.

³³ Los cargos son realizados de manera directa en la cuenta que el comprador tiene establecida en una entidad de crédito, destacando los pagos que se realizan por medio de domiciliación bancaria, tarjeta de débito y cheque electrónico.

³⁴ Con el término esquema se hace referencia a los concretos sistemas de dinero electrónico objeto de diseño o implementación.

³⁵ Por medio de su domiciliación en su cuenta corriente o su inclusión en la factura de las operaciones realizadas por medio de tarjeta de crédito, o bien, en el caso de aquellos sistemas que añaden a transacciones realizadas a la factura de teléfono del comprador.

b) Sistemas de pago por medio de teléfonos móviles³⁷ u otros terminales inalámbricos³⁸. Este es uno de los terrenos que mejor puede servir al desarrollo de los nuevos instrumentos de pago electrónico por cuanto el nivel de penetración de este tipo de terminales es incluso más elevado que el relativo a los ordenadores personales³⁹.

³⁶ Los sistemas de micropagos están específicamente diseñados y pensados para su exclusiva aplicación a los pagos realizados a través de la red de redes. Parecen abocados a satisfacer una nueva necesidad que viene impuesta por la propia naturaleza de la información y servicios que pueden proporcionarse a través de Internet. En este sentido, *vid.* ASOKAN, N., JANSON, P. A., STEINER, M., WAIDNER, M., en *The State of the Art in Electronic Payment Systems*, IBM Zurich Research Laboratory, septiembre, 1997.

³⁷ La generalización del teléfono móvil en estos últimos años ha llevado a algunas empresas telefónicas, ante la necesidad de un sistema de pago seguro y rápido, a desarrollar sistemas basados en el habitual teléfono móvil. La primera experiencia europea en este sentido se ha producido en Italia de la mano de la compañía Omnipay <<http://www.omnipay.it/>>, a la que, a efectos expositivos, tomaremos como ejemplo. El usuario de este medio de pago puede optar por dos opciones: a) Un sistema de pago basado en tarjetas prepago (a imagen de las populares tarjetas telefónicas). b) Otro, en cargo indirecto a la tarjeta de crédito del usuario, previa confirmación telefónica del pago. El sistema de pago móvil basado en tarjetas prepago es especialmente sencillo. El usuario adquiere una tarjeta prepago en cualquiera de los establecimientos autorizados por la compañía prestadora del servicio. Elegido el comerciante, en Internet o en cualquier otra red abierta que admita este tipo de pago, y el producto deseado, el usuario presionará el icono de la empresa suministradora del servicio de pago. En ese momento se inicia una conexión segura con la empresa suministradora del servicio de pago, la cual solicitará al usuario que introduzca las catorce cifras del código secreto incluido en la tarjeta prepago. De esta forma, la empresa suministradora del servicio de pago conocerá el importe total del que el usuario es acreedor, procediendo a autorizar el pago si el precio del bien o del servicio es inferior al saldo remanente en la tarjeta prepago. Autorizado el pago, el titular recibirá una factura electrónica en la que se le indicará la información acerca del bien adquirido y el precio que por él se ha efectuado. Este sistema tiene ventajas indudables: Es seguro, confidencial, anónimo y completamente electrónico. No obstante no es una solución global, ya que los comerciantes deben admitir el pago y celebrar contratos de adhesión con cada una de las compañías que ofrecen este servicio, por lo que el usuario sólo puede pagar por este medio en un limitado número de comercios y no, como ocurre en los pagos con tarjeta, en la mayoría absoluta de los establecimientos virtuales. Por otra parte, es un medio destinado a satisfacer pagos de escasa monta, siendo una solución válida y eficaz al problema de los micropagos pero haciendo imposible el pago de bienes y servicios de importe elevado. El pago de bienes y servicios de coste elevado, sin embargo, es solventado mediante ésta el pago móvil basado en el pago indirecto con tarjeta de crédito. No obstante, al contrario que en el supuesto anterior, éste medio de pago no se realiza únicamente en la red, lo que lo desvirtúa, en buena medida, como medio de pago. El procedimiento es el siguiente. Es necesario convertirse en titular de una tarjeta de crédito. En el caso de la empresa tomada como ejemplo, ésta obliga al usuario a suscribir una tarjeta de crédito en concreto: La *Visa Bank Americard Omnitel* <<http://www.omnipay.omnitel.it/modulo.htm>>. Suscrita la cual el titular recibe, además de la titularidad y la clave común a todas las tarjetas bancarias, el PIN necesario para confirmar telefónicamente los pagos deseados. Elegido el comerciante y el producto, se selecciona el pago móvil como modalidad de pago. A continuación se introduce el número

c) Sistemas de prepago. Por medio de los cuales el usuario transfiere un determinado valor a una cuenta personalizada en poder del proveedor de servicios de pago o a un determinado aparato que bien puede consistir en una tarjeta inteligente⁴⁰, un ordenador personal u otro de similares características. Nos referimos al *personal on-line payment services*⁴¹, al dinero electrónico⁴², monederos electrónicos⁴³.

del teléfono y se confirma que se desea efectuar el pago. Finalmente y dentro de un periodo de 24 horas, el usuario debe comunicarse telefónicamente con la empresa suministradora del servicio de pago para confirmar, mediante la comunicación del PIN, la autorización del pago. Efectuada la confirmación, la empresa autoriza y hace efectivo el pago por los medios tradicionales de pago con tarjeta. Como se observa, esta segunda modalidad, si bien hace posible el pago de importes elevados, presenta serios inconvenientes. Es una solución que sigue sin ser global. El usuario sólo tiene la posibilidad de contratar con los comercios adheridos a la empresa prestadora del servicio de pago. No es confidencial ya que todos los intervinientes en el pago conocen el precio y el bien o el servicio contratado. Tampoco es anónimo, pudiendo el banco elaborar un perfil de los gustos y hábitos del comprador.

³⁸ Las tecnologías aplicadas al nuevo sector de las comunicaciones inalámbricas han provocado la aparición de nuevos aparatos o terminales, más allá de los clásicos teléfonos móviles, sobre los que se implementan aplicaciones y protocolos, como el ya superado WAP (*Wireless Application Protocol*), el GPRS (*General Packet Access Service*) o el UMTS (*Universal Mobile Telecommunication Services*), relativo a la tercera generación de comunicaciones inalámbricas. Vid. en este sentido, MATEO HERNÁNDEZ, J. L., "El WAP: Aspectos jurídicos y principales interrogantes en el terreno de la contratación", *XIV Encuentros sobre Informática y Derecho*, Instituto de Informática Jurídica, Universidad Pontificia de Comillas, Aranzadi, Madrid, 2000, pp 471 a 482, e IGLESIAS PORTELA. M. J. y MATEO HERNÁNDEZ, J. L., "M- Commerce: Contract Law, Electronic Payment and Consumer Protection", fruto de la celebración en mayo de 2001 del ECLIP M- Commerce Forum en Palma de Mallorca. *ECLIP Series, IST Project 1999- 12278, Electronic Commerce Legal Issues Platform II, 2002*.

³⁹ Así, ya se han diseñado y vienen utilizándose diversos sistemas por medio de los cuales puede iniciarse un pago haciendo uso de mensajes de texto o SMS (*Short Messages System*), o bien autorizarse la relación del pago por medio de llamadas de teléfono al portador del Terminal.

⁴⁰ La naturaleza cambiante de los Medios de Pago se está viendo acelerada en estos últimos años por la introducción de nuevas tecnologías que cambian drásticamente el modo en que nos relacionamos, operamos e interactuamos en general con nuestro entorno. Estas nuevas tecnologías y, concretamente, las tarjetas inteligentes e Internet, están abriendo nuevos entornos de productos pero, al mismo tiempo, introducen nuevos riesgos (o niveles de riesgos) en el sistema. En el caso de las tarjetas inteligentes nos encontramos ante una tecnología que, con productos diseñados e implantados de la manera apropiada, nos puede proporcionar una oportunidad incomparable para mitigar y, potencialmente, eliminar algunos de los problemas de fraude con los que actualmente nos enfrentamos. Hay dos puntos de vista diametralmente opuestos acerca de la seguridad de las tarjetas con microprocesador: que son inherentemente seguras y que se "rompen" fácilmente. Entendemos que ninguno de los dos es correcto. Hay algunos casos, que han sido objeto de gran atención por parte de la prensa, en los que se habla de tarjetas inteligentes que han sido "rotas", pero si la tarjeta ha sido diseñada con el objetivo de mantener

la seguridad puede ser muy difícil de atacar. Todos podemos asegurarnos de que nuestra tarjeta está al nivel adecuado si comprendemos cuales son las amenazas y tomamos las medidas necesarias para contrarrestarlas. Algunas tarjetas son más susceptibles a los ataques que otras. Hay una serie de medidas de seguridad perfectamente conocidas que pueden añadirse a los microprocesadores de las tarjetas "chip" o a las aplicaciones, pero no siempre son utilizadas o activadas. Los "chips" que han sido utilizados tradicionalmente en las tarjetas inteligentes fueron diseñados en su origen como microcontroladores incrustados y además son utilizados en una amplia variedad de aplicaciones donde la seguridad no es un problema. De hecho, la seguridad puede ser innecesaria en estas otras aplicaciones, porque fueron diseñadas para entornos de alta fiabilidad. Esto quiere decir que si algo va mal, el "chip" tratará de solventar el problema y continuará "haciendo lo que ha sido diseñado para hacer". Pero en una tarjeta inteligente, ese problema puede ser un signo de que un "hacker" está intentando obtener información confidencial de la tarjeta. Lo que necesitamos de ese "chip" es que "falle" limpiamente con un "reset" o un bloqueo total, dependiendo del tipo y la gravedad del ataque. No hay manera de garantizar la seguridad, pero la mejor manera de asegurarse un nivel alto de seguridad es tener el diseño evaluado y el producto final probado. Dado que las capacidades de análisis y prueba mejoran constantemente, es imposible prever todos los ataques que alguien pueda imaginar. Diseñar con la seguridad en mente agrega complejidad y costo a los "chips". En algunas aplicaciones de alta seguridad, el riesgo de que alguien pueda obtener una información puede ser lo suficientemente alto como para necesitar asegurarse de que todas las medidas de seguridad posibles han sido implantadas. En un mundo ideal las tarjetas de servicios financieros serían una de estas aplicaciones. Pero la industria financiera es muy sensible a los costes. Las tarjetas de banda magnética funcionan bastante bien para su uso actual y, si las tarjetas inteligentes van a sustituirlas en algún momento, el precio debe ser tan bajo como sea posible. Hay una variedad de estándares internacionales que algunos pueden pensar que garantizan la seguridad de las tarjetas inteligentes financieras. Sin embargo, muchos de ellos, como ISO 7816, se refieren a la funcionalidad de las tarjetas más que a su seguridad. No se puede depender únicamente de estos estándares para garantizar ningún nivel de seguridad en particular. ITSEC (*Information Technology Security Evaluation Criteria*) es un sistema europeo desarrollado para validar aspectos de seguridad en las tecnologías de la información. ITSEC se ocupa de verificar aquello que ha sido declarado por el fabricante del producto, a través de laboratorios independientes y licenciados. Sin embargo, las declaraciones no están estandarizadas. Así, si un producto tiene una calificación ITSEC, esto no nos indica por sí mismo que ha sido declarado y validado en su totalidad. La validación puede haberse realizado únicamente en una parte del sistema, por ejemplo el generador de números aleatorios. Aunque tener un buen generador de números aleatorios es una característica de seguridad importante en un "chip", esto no nos dice nada acerca de otras características que pueden conllevar vulnerabilidades significativas. ITSEC es un paso en la dirección correcta, pero no es suficiente en sí mismo. Existe asimismo una variedad de estándares de seguridad gubernamentales en diversos países, pero no son consistentes entre sí. Algunos gobiernos requieren que todos los sistemas de monedero electrónico sean auditables, otros no. Algunos requieren cifrado DES en determinados puntos, otros 3-DES, tecnologías de clave pública o cualquier otra forma de cifrado específica. Cualquier certificación de que una tarjeta inteligente en particular cumple los estándares de seguridad de un gobierno, no significa necesariamente que sea aceptable en cualquier otro lugar. El esfuerzo que se está llevando a cabo bajo el nombre "Common Criteria" (*Common Criteria for Information Security Technology*) tiene un enorme interés. A pesar de ello, no incluye a todos los países con cierta significación en la industria (entre ellos España), y precisa de algunos ajustes operativos para satisfacer no sólo las necesidades de los fabricantes sino también las de los usuarios. Los requerimientos de la industria financiera son algo diferentes de los del resto. Las tarjetas telefónicas, por ejemplo, GSM o prepagadas,

d) Tarjetas virtuales. Las tarjetas para pagos en Internet representan la última novedad en materia de tarjetas electrónicas. Aún cuando para el pago en el comercio electrónico en Internet no es necesaria la configuración de una tarjeta especial en el sentido que podemos pagar con las tradicionales tarjetas de crédito, débito o compra, las numerosas reclamaciones de los clientes por el uso fraudulento de las tarjetas, impulsaron a las diferentes instituciones financieras y

están diseñadas para ser usadas siempre en conexión, mientras que las tarjetas financieras necesitan en determinadas circunstancias operar fuera de línea. Estas diferencias se traducen en diferentes requerimientos de seguridad y diferentes mecanismos de protección. Los requerimientos de la televisión de pago son también diferentes. La industria del cable estima que una parte significativa de su beneficio potencial se pierde a causa de los "piratas" que roban la señal sin pagar por ella. Pero siempre se trata de una pérdida de beneficio potencial, no real. Un sistema de tarjeta inteligente que capture incluso una pequeña proporción de este beneficio potencial es una ganancia neta para su sistema, con un pequeño coste adicional. En cambio, cada vez que una tarjeta bancaria es utilizada, hay una transferencia de fondos. Alguien tiene que responder por cada transacción fraudulenta; conlleva una pérdida de ganancia real, no potencial. Las amenazas, requerimientos de seguridad y mecanismos de auditoría del sistema son, por consiguiente, diferentes. En el otro extremo, las tarjetas utilizadas para proteger bienes extremadamente valiosos, como redes de seguridad nacionales, pueden diseñarse para autoborrarse al detectar el menor signo que indique un potencial ataque exterior. Eso tampoco funcionaría con una tarjeta financiera. En ambos casos hay procedimientos de respaldo para proteger el acceso del usuario a sus fondos, pero las situaciones son muy diferentes. En un sistema financiero la tarjeta es parte de un sistema más grande que incluye simultáneamente debilidades y medidas de protección adicionales. En transacciones de crédito y débito existe un extracto mensual que el titular puede revisar para detectar errores. Los establecimientos comerciales que cometen "errores" con excesiva frecuencia pueden ser incluidos en una lista de alertas y educados o corregidos de diversas maneras. El sistema puede tolerar errores aislados porque aún pueden manejarse de manera razonable y rentable. Ciertas aplicaciones de seguridad nacional, en cambio, no pueden tolerar ni un solo error. La mayoría de los sistemas de telecomunicaciones, por otro lado, no pueden depender de un extracto mensual para detectar y corregir errores. Cada industria y cada aplicación tiene sus propios requerimientos de seguridad, así que es difícil que exista un estándar de seguridad único. Lo que es importante es comprender el rol que juega la tarjeta en la globalidad del sistema al que pertenece, y diseñar la seguridad que es adecuada y apropiada para ese rol. Las tarjetas inteligentes dependen generalmente de la criptografía para al menos parte de su seguridad. Los conocimientos de criptografía y la capacidad para la misma son diferentes de los requeridos para el "hardware" y el "software". La criptografía requiere un talento especial. En este sentido, GINEL, F., "Seguridad en Tarjetas con Microprocesador: Procedimientos de Evaluación y Consecución de Estándares", *Publicado en el Boletín del Criptonomición # 47 y # 49.*

⁴¹ Se caracteriza por posibilitar la conclusión de pagos entre particulares (*person-to-person e-payments*) a través de Internet, haciendo uso de los correos electrónicos y de la propia página del proveedor de servicios de pago para la formalización de las diversas comunicaciones e intercambios de información del pago.

⁴² Conforme a lo establecido en la *Directiva 2000/46/CE, del Parlamento Europeo y del Consejo, de 18 de septiembre, sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades*, concretamente en su artículo 3b) se define como "un valor monetario

propietarias de las marcas que emiten las tarjetas a trabajar en el diseño de tarjetas especiales para su uso específico en Internet.⁴⁴

En Italia se está implantando el sistema de pago mediante lectores de tarjetas conectados al PC del comprador. Se trata de un sistema que permite hacer los pagos en Internet sin enviar el número de la tarjeta de manera que ningún *hacker*⁴⁵ pueda apropiarse de los datos del instrumento de pago ni descifrar los algoritmos matemáticos de cifrado de la información.⁴⁶

representado por un crédito exigible a su emisor: i) almacenado en un soporte electrónico, ii) emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido, iii) aceptado como medio de pago por empresas distintas del emisor". Dicho valor figurará, bien en la memoria de un ordenador o aparato de similares características, dando lugar a los denominados *softwares based e-money schemes*; o en una tarjeta, refiriéndonos en este caso a los *card based e-money schemes*.

⁴³ Los monederos electrónicos son tarjetas de prepago que permiten almacenar unidades monetarias en un microchip con la finalidad de realizar pequeñas compras, (cabinas telefónicas, taxis, kioscos, bares, pequeños comercios de alimentación) donde hasta ahora no se aceptaba la tradicional tarjeta de crédito y el consumidor debía realizar los pagos en efectivo. El funcionamiento de los monederos electrónicos implica el almacenamiento -previo a su uso- de una determinada cantidad de dinero a voluntad del titular de la tarjeta mediante una transferencia de la cuenta bancaria del usuario del monedero. Con el dinero contenido en el monedero electrónico, el titular puede adquirir los productos y servicios de los proveedores adheridos al sistema, el uso de esta tarjeta implica su introducción en el dispositivo adecuado del proveedor de bienes y/o servicios a objeto de registrar la operación realizada y efectuar la correspondiente deducción del saldo, situación que en principio limita el uso de la tarjeta monedero en operaciones en Internet, no obstante su uso se está implantando a través de la instalación de un hardware específico en los ordenadores de los usuarios que permite la lectura de las tarjetas. El importe de las operaciones se registra tanto en la tarjeta a través de microchip, como en los registros informáticos del banco. La utilización del monedero electrónico comporta para el titular la asunción de los riesgos en caso de utilización fraudulenta o irregular así como por su pérdida, incluso después de haberlo notificado al banco. Entre los principales sistemas de pago que utilizan el monedero electrónico cabe mencionar el Sistema de Europay, MasterCard y Visa (EMV), el *European Electronic Purse* (EEP), iniciativa del *European Committee for Banking Standards* (ECBS), el *Conditional Access for Europe* (CAFE) el sistema MONDEX y el *CyberCash*, una de las tarjetas monedero que lleva más tiempo en el mercado es la tarjeta creada por la empresa Mondex, subsidiaria de MasterCard, esta tarjeta permite almacenar distintas divisas y contiene un programa de seguridad para proteger el dinero contenido en el monedero electrónico. Las tarjetas monedero se presentan como una posible solución al problema de los micropagos (pagos de pequeñas cantidades cuyo abono por tarjeta genera unos costes excesivamente altos para el consumidor), y si bien su uso presenta ventajas indudables, también halla serios escollos en su camino: a) Este tipo de tarjetas monedero permite realizar pagos como si poseyéramos un monedero real, es decir, podemos portar pequeñas cantidades de dinero, gozar de anonimato en las formas de pago, aceptación del valor monetario almacenado en un territorio amplio y determinado, ventajas todas ellas atractivas para el consumidor que ve posibilitado el cumplimiento de pagos sin llevar dinero físico con todas las ventajas de éste y a un coste cero o muy bajo. b) Como antes se advertía, no todo son ventajas. Los tipos de tarjetas

Los medios de pago tradicionales sufren numerosos problemas de seguridad: falsificación de billetes, falsificación de firmas, cheques sin fondo, etc. Por otro lado, los medios de pago electrónicos, además de estar sujetos a los mismos problemas anteriores, presentan riesgos adicionales, pues a diferencia del papel, los documentos digitales pueden ser copiados perfectamente y cuantas veces se desee, las firmas digitales pueden ser falsificadas por cualquiera que conozca la clave privada del firmante, la identidad de una persona puede ser asociada de forma inequívoca con la información relacionada en cada pago, etc.

Es por ello que es necesario establecer nuevos mecanismos de seguridad para los nuevos medios de pago electrónicos si se quiere que tanto las entidades bancarias como los usuarios finales acepten de forma generalizada estos nuevos

monedero, emitidas por las diferentes entidades bancarias, son diversos y, en múltiples ocasiones, incompatibles entre sí, lo que limita su uso a aquellos comercios en los que la entidad bancaria, emisora de la tarjeta, y la del lector, cedido al comercio, fuera la mismo. Por ello, esfuerzos destinados a la búsqueda de la compatibilidad de estas tarjetas es un reto que las entidades bancarias deben marcarse si desean, como parecen querer hacerlo, que esta tecnología se imponga.

⁴⁴ En España, Banesto ha sido la institución pionera en lanzar al mercado la denominada "Virtual Cash", se trata de un monedero electrónico de uso exclusivo para Internet, diseñado para efectuar pequeños pagos, la tarjeta no incorpora microchips, ni bandas magnéticas, sólo un número que sirve para cargarla en el cajero, tampoco está vinculada a una cuenta corriente y se puede solicitar *on line*, en la página Web de Banesto, su funcionamiento se basa en un número asignado a la tarjeta y la clave secreta que se utiliza para el recargo con la tarjeta de crédito o débito del cliente, y es aceptada en los establecimientos afiliados al sistema VirtualCash.

⁴⁵ Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar *hackeo* y *hackear* a las obras propias de un hacker. El término "Hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. Hacker, usando la palabra inglesa, quiere decir divertirse con el ingenio [cleverness], usar la inteligencia para hacer algo difícil. No implica trabajar solo ni con otros necesariamente. Es posible en cualquier proyecto. No implica tampoco hacerlo con computadoras. Es posible ser un hacker de las bicicletas. Por ejemplo, una fiesta sorpresa tiene el espíritu del hack, usa el ingenio para sorprender al homenajeado, no para molestarle.

⁴⁶ El sistema es proporcionado por la empresa Mover, especializada en diseños de sistemas de seguridad para pagos electrónicos. Mediante un acuerdo contractual que incluye el pago correspondiente al servicio, la empresa expide directamente al usuario un kit compuesto de una tarjeta inteligente denominada *Movercard* y un lector para conectar al PC. La firma electrónica del usuario está contenida en el microprocesador de la tarjeta de modo que es posible reconocer su identidad, una vez insertada la tarjeta en el lector se teclea el PIN y se autoriza el pago, con este sistema es posible hacer compras en los establecimientos afiliados al sistema Mover.

medios de pago. Por otro lado, si los sistemas de pago electrónicos son bien diseñados, pueden proporcionar una mayor seguridad y flexibilidad de uso que la ofrecida por los medios de pago tradicionales.

La criptografía está desempeñando un papel fundamental en la incorporación de nuevos medios de pago a los ya existentes hoy en día, pues es la base sobre la que se sustenta la seguridad de estos nuevos medios. Por otro lado, la aparición de nuevos dispositivos físicos como las tarjetas inteligentes y otros módulos de seguridad permite y posibilita la implementación de los diferentes protocolos criptográficos de estos medios de pago.

España es uno de los países pioneros en la adopción de nuevos medios de pago y nuevas tecnologías como lo demuestran la presencia de la tarjeta monedero (p. ej., la Visa Cash) en el mercado desde hace ya años y la implantación de los sistemas de pago a través de Internet. En un futuro próximo los españoles veremos además como nuestras tradicionales tarjetas de crédito y débito, que tradicionalmente operan a través de una banda magnética, serán sustituidas por tarjetas inteligentes con los más populares algoritmos criptográficos y que podrán contener además, cualquier tipo de aplicación financiera.

e) Títulos Valores Electrónicos. En sus orígenes, la noción del título-valor electrónico se identificaba con el efecto producido como consecuencia de la desmaterialización del título valor, fenómeno que permite la circulación electrónica de los títulos gracias a anotaciones contables en un soporte electrónico. Si bien este proceso contribuyó a la agilización de los títulos-valores en masa (acciones y obligaciones), no resultaba del todo idóneo para los títulos emitidos individualmente como es el caso de la letra de cambio y el cheque. Actualmente se habla de “electronificación de los títulos valores”⁴⁷ aludiendo esta frase, tanto al sistema de desmaterialización tradicional, como a la emisión y circulación electrónica a través de redes de títulos cambiarios susceptibles de uso como medios de pago, en este caso, nos referimos a letras de cambio y cheques electrónicos.

- Letras de cambio electrónicas: La emisión electrónica de letras de cambio es perfectamente factible en los países que no exigen la utilización de formatos específicos para su emisión⁴⁸. La mayoría de los países que han adoptado legislación en materia de contratación y comercio electrónico consagran el

⁴⁷ En tal sentido, ILLESCAS ORTÍZ, R., *Derecho de la contratación electrónica*, Civitas, Madrid, 2001 y RECALDE CASTELLS, A., “La electronificación del título-valor”, ponencia presentada en las II Jornadas de Derecho del Comercio Electrónico. Universidad Carlos III de Madrid, mayo, 2001.

principio de equivalencia funcional entre el documento electrónico y el documento que requiere el tradicional soporte en papel, de igual manera que consagran el principio de equivalencia funcional entre la firma autógrafa y la firma manuscrita. El principal problema que se suscita con el uso electrónico de la letra de cambio, es el mismo que se presenta en la actualidad con el uso de la letra de cambio tradicional por efecto del fenómeno conocido como “la crisis de la letra de cambio” derivado principalmente de la pérdida de confianza en el instrumento cambiario.

- Cheques electrónicos: En materia de cheques electrónicos susceptibles de uso en Internet, existen en la actualidad dos proyectos oficiales: el proyecto FSTC (*Financial Services Technology Consortium*) en Estados Unidos y el Proyecto MANDATE (*Managing and Administrating Negotiable Documents and Trading them Electronically*) en Europa. Al lado de estos proyectos existen diversas iniciativas de las grandes empresas y compañías informáticas para facilitar el pago de las compras a través de Internet en los que cabe resaltar el uso de Net Check, el Cashier Check y el Check Free.

En líneas generales, el funcionamiento de los citados proyectos se basa en la sustitución del soporte tradicional del cheque -el papel- por un soporte electrónico que permite emitir y enviar el cheque al tenedor a través de la Red; de igual forma, el tradicional talonario de cheques se sustituye por una chequera electrónica de bolsillo contenida en una tarjeta electrónica. La seguridad de estos sistemas se basa en el uso de algoritmos criptográficos que permiten garantizar la integridad de los datos contenidos en el cheque, evitar las duplicaciones y mantener oculto el número de cuenta del librador.

El uso del cheque electrónico debe ser pactado con el banco o entidad financiera y debe insertarse dentro del contrato de cuenta corriente de igual forma como se pacta el uso del cheque tradicional ya que en virtud de este contrato es que la entidad se obliga a satisfacer al tenedor el importe del cheque. Debe existir una cláusula en el contrato que permita la emisión de cheques mediante el uso de la firma electrónica registrando los datos relativos a la firma del librador tal como se hace en los casos de las firmas manuscritas, para lo cual será necesario la

⁴⁸ En España, la emisión de la letra de cambio está sujeta a lo dispuesto en el texto refundido de la Ley de Impuesto sobre transmisiones patrimoniales y actos jurídicos documentados de 24 de septiembre de 1993, en cuyo artículo 37 se establece la necesidad de extender la letra en el efecto timbrado de la clase que corresponde a su cuantía, según esto, la letra de cambio solo vale como tal si está confeccionada de acuerdo al modelo oficial vigente expedido por la Fábrica Nacional de Moneda y Timbre.

intervención de una tercera parte, el prestador de servicios de certificación a efectos de certificar los datos relativos a la firma electrónica del librador⁴⁹.

El sistema del *E-check* permite la emisión de cheques certificados mediante la certificación bancaria del instrumento, este procedimiento se lleva a cabo a través de la inserción de parte de la institución financiera de un sello de garantía avalado con su firma electrónica, garantizando al portador del cheque la existencia de una determinada disponibilidad a su favor, de esta manera funciona el sistema "Cashier Check", utilizado con mayor difusión en Estados Unidos.

Los requisitos de seguridad pueden variar ligeramente de un sistema de pago a otro dependiendo tanto de las características propias del sistema como por la confianza que exista entre los diferentes elementos del mismo. Así, un sistema de pago realizado en un entorno en el que las comunicaciones se realizan a través de una red de área local o metropolitana sin salir al exterior, no requiere el mismo nivel de seguridad que un sistema de pago en el que las transacciones se envían a través de Internet, pudiendo recorrer el mundo entero.

En cualquier caso, podemos decir que los requisitos de seguridad de un sistema de pago electrónico en general son los siguientes:

a) Autenticación: En todo sistema de pago los participantes del sistema deben demostrar que son los que dicen ser. Así, en un sistema de pago basado en tarjetas de crédito, el comercio comprueba la autenticidad de la tarjeta antes de proceder con el pago. En el caso de tarjetas inteligentes (con microprocesador, dotadas por tanto de una capacidad de cálculo) ésto se realiza mediante algún protocolo criptográfico de autenticación, mientras que en el caso de tarjetas con banda magnética, se realiza mediante una verificación visual de ciertos datos grabados en la superficie de la tarjeta (hologramas, firmas, etc.). En el caso de sistemas de pago basados en monederos electrónicos es frecuente también que se produzca una autenticación del comercio ante el portador del monedero electrónico debido al riesgo existente de creación de dinero falso en este tipo de sistemas. Para ello el terminal del comercio suele disponer de un módulo de seguridad, que en ocasiones es una tarjeta inteligente pero puede ser otro tipo de dispositivo, el cual almacena las claves y realiza los cálculos necesarios para la autenticación del comercio.

En los sistemas basados en tarjetas se suele verificar también la asociación correcta de la tarjeta con su poseedor (titular de la cuenta asociada a la tarjeta). Esto se realiza normalmente a través de números de identificación personal (PIN).

⁴⁹Un tratamiento más profundo sobre el funcionamiento del cheque electrónico puede consultarse en RAMOS HERRANZ, I., en "Cheques electrónicos", *Revista de Derecho Mercantil*, 1998.

Lo mismo ocurre en los sistemas de pago a través de redes donde se necesita una autenticación de la persona física que utiliza en un instante determinado el sistema.

La autenticidad del resto de agentes de un sistema de pago electrónico es normalmente garantizada mediante protocolos criptográficos de autenticación, actualmente basados en algoritmos de clave simétrica como el DES, pero que poco a poco están siendo remplazados por algoritmos de clave pública como el RSA con el fin de favorecer la interoperabilidad de los sistemas.

b) Integridad: Otro aspecto importante en todo sistema de pago electrónico es la integridad de los datos intercambiados entre los agentes del sistema, máxime cuando esos datos se refieren a importes de un pago, a un número de cuenta bancaria, etc. La integridad de las comunicaciones se garantiza mediante códigos de autenticación de mensajes (MACs), funciones resumen y firmas digitales. En el caso de la relación cliente - comercio, esto sólo es posible cuando el cliente está en posesión de un dispositivo con capacidad de cálculo y de almacenamiento seguro de claves, como es el caso de una tarjeta inteligente.

Además, es también importante salvaguardar la integridad de los datos almacenados en los dispositivos asociados a cada agente. Las claves criptográficas, los certificados, las listas negras, los datos para el intercambio de operaciones, etc., necesitan ser protegidos contra la alteración voluntaria o involuntaria de los mismos. Esto se consigue de muy diversas maneras según el tipo de agente y según el dispositivo asociado a él. Así por ejemplo, las claves criptográficas de clientes y comercios suelen almacenarse en tarjetas inteligentes y módulos de seguridad (SAMs) respectivamente. Las listas negras en los comercios se verifican y renuevan periódicamente y los datos en los servidores de las entidades financieras que intervienen en el sistema de pago que son almacenados en búnkers de seguridad que normalmente se encuentran duplicados para evitar las posibles pérdidas de información como consecuencia de posibles fallos.

c) Confidencialidad: Ciertos datos intercambiados durante una transacción de pago necesitan ser ocultados a la vista de todo el mundo salvo para el agente al que van destinados dichos datos. Es el caso de la información asociada con la cuenta bancaria de un titular que se transmite a través de una red y que sólo concierne al titular y a la entidad bancaria depositaria de dicha cuenta. También ciertos datos asociados con los bienes o servicios adquiridos son susceptibles de ocultación en cuanto a que pueden constituir datos sensibles que en manos de terceros pudieran causar un grave perjuicio directo o indirecto al cliente.

La confidencialidad se garantiza normalmente mediante el cifrado de datos. Sin embargo, ésta cuestión está resultando ser un problema en la mayoría de los países debido a las restricciones impuestas por los diferentes gobiernos para utilizar algoritmos criptográficos de cifrado de datos con un alto nivel de seguridad. En algunos países (Francia) el cifrado de datos está absolutamente prohibido sin el permiso de la oficina gubernamental correspondiente y normalmente sin el depósito previo de las claves de cifrado en dicha oficina. En otros países (EEUU) se restringe la utilización de estos algoritmos al territorio nacional, debiendo utilizar una versión mermada del algoritmo si se quiere utilizar más allá de sus fronteras.

En ciertos casos se requiere que el pago se realice de forma anónima de tal modo que sea imposible a partir de ciertos datos, elaborar una traza que permita descubrir el autor de un determinado pago. Estos sistemas requieren protocolos criptográficos más complejos cuando el pago se realiza a través de una cuenta bancaria, pues los datos del titular son almacenados en el momento de la autorización del pago o de la retirada de dinero (en el caso del monedero electrónico). Actualmente el anonimato es garantizado en todas aquéllas transacciones que se realizan con dinero no ligado a una cuenta bancaria, como por ejemplo las tarjetas de prepago en las cabinas telefónicas.

d) Prueba de la transacción: Cuando se produce una transacción electrónica en la que una cantidad de dinero se mueve de un agente a otro de la transacción es necesario una prueba de la misma que permita al pagado reclamar ese dinero y evite que el pagador reniegue del pago. Generalmente, el banco depositario de la cuenta del cliente (banco emisor) debe pagar una determinada cantidad de dinero al banco depositario de la cuenta del comercio (banco adquirente) por las transacciones llevadas a cabo en sus terminales. El banco emisor reclamará entonces una prueba de que dichas transacciones fueron efectivamente realizadas por titulares de cuentas de ese banco y por el importe reclamado.

La prueba de la transacción suele ser realizada por el cliente en los casos en que éste dispone de un dispositivo con capacidad de cálculo (tarjeta inteligente, PC, etc.). Suele consistir en una firma digital realizada mediante algún algoritmo de clave pública con el fin de evitar la repudiación de la prueba. Sin embargo, puesto que en la mayoría de los sistemas de pago electrónico existe una relación bilateral de responsabilidades entre el titular y el banco emisor de la tarjeta del titular, la prueba de la transacción suele consistir en un MAC con funciones de firma digital, generado con un algoritmo de clave simétrica en el que la clave es compartida por

el titular de la cuenta (cliente) y el banco emisor, con el fin de reducir el tiempo de cálculo y el número de datos enviados a este último.

e) Gestión del riesgo y autorización: Otro aspecto muy importante a la hora de autorizar o no un pago es realizar una estimación del riesgo que supondría autorizar un pago fraudulento. Para ello, todos los agentes que intervienen en el momento de realizarse la transacción realizan un análisis de la situación en la que la transacción se produce con el fin de autorizar el pago o no. En este caso tenemos dos situaciones bien distintas, según la autorización se realice directamente por el banco emisor tras una conexión en línea con el comercio, o se realice por otro agente y sin conexión con el banco emisor (fuera de línea).

En el caso de autorizaciones en línea, el banco emisor puede verificar directamente la autenticidad del cliente (por ejemplo, mediante una verificación del PIN en los sistemas actuales de retirada de dinero con tarjeta en cajeros automáticos) y puede consultar los datos de éste (listas negras, saldo disponible, límites establecidos, etc.) para autorizar el pago o no.

En el caso de autorizaciones fuera de línea, no se conoce exactamente la situación financiera del cliente, por lo que se tiene que realizar una estimación del riesgo basada en el análisis de algunos parámetros como por ejemplo, el importe de la transacción, la procedencia (nacional, comunitaria, extranjera) del cliente, consultar listas negras actualizadas periódicamente por las diferentes entidades bancarias emisoras, etc. Normalmente este tipo de autorizaciones resultan mucho más económicas debido al ahorro en la llamada telefónica solicitando la autorización, pero conllevan un mayor riesgo y exigen por tanto unos protocolos criptográficos más robustos que permitan al comercio autenticar al cliente sin necesidad de consultar a su banco.

f) Disponibilidad y fiabilidad: Todas las partes implicadas en un sistema electrónico de pago requieren la habilidad para realizar o recibir pagos cuando sea necesario. Por otro lado, las transacciones deben ser atómicas, en el sentido de que o se producen satisfactoriamente o no se producen, pero no pueden quedar en un estado desconocido o inconsistente. Ningún cliente o comercio aceptaría una pérdida de dinero por culpa de un error en el sistema. La disponibilidad y la fiabilidad del sistema dependen de la disponibilidad y fiabilidad de los dispositivos y de las redes sobre las que se sustenta. La recuperación ante fallos requiere un sistema de almacenamiento estable en todas las partes del sistema y protocolos específicos de sincronismo.

5. EL DINERO ELECTRÓNICO⁵⁰

5.1. PLANTEAMIENTO GENERAL

No existe una única definición ni un concepto claro y mayoritariamente aceptado de dinero electrónico⁵¹, y como advirtió en su momento el Comité Económico y Social Europeo, esta figura no puede ser percibida como un instrumento de pago más, sino el instrumento de pago del futuro en el comercio electrónico por Internet⁵².

Es necesario acudir al concepto mismo de dinero, su origen y evolución para alcanzar una idea completa de esta nueva realidad que cobra especial relevancia con las ya concurrentes autopistas de la información⁵³. En la actualidad existen diversas formas de dinero, es decir, diversas manifestaciones que sirven como dinero y pueden agruparse en tres bloques: dinero efectivo⁵⁴ y dinero contable⁵⁵. Pues bien, dentro del proceso denominado digitalización del dinero⁵⁶ el dinero electrónico queda enmarcado como sustituto digital del dinero efectivo, denominado por algunos autores como dinero efectivo electrónico⁵⁷.

El dinero electrónico es dinero efectivo en formato electrónico, de modo que

⁵⁰ Lo realmente esencial de este medio de pago es que no representa un bien en sí mismo, sino en cuanto es objeto de un reconocimiento social y de una significación jurídica. En palabras de DÍEZ PICAZO, "el dinero adquiere su sentido porque existe una normativa que lo establece como medio general de cambio y como unidad de valor, pero también porque una determinada comunidad o grupo humano le otorga su confianza y admite en general su vigencia". Vid. DÍEZ PICAZO, L., *Fundamentos del Derecho Civil Patrimonial*, ..., *op. cit.* pág. 256.

⁵¹ Vid. GALBRAITH, J. K., *El dinero*, Editorial Ariel, Barcelona, 1996, pág. 13, que advierte de la dificultad de alcanzar una acertada definición teórica de dinero.

⁵² Dictamen del Comité Económico y Social Europeo sobre la *Propuesta de Directiva del Parlamento Europeo y del Consejo sobre el inicio, el ejercicio y la supervisión cautelar de las actividades de las entidades de dinero electrónico* y la *Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva 77/780/CEE sobre la coordinación de las disposiciones legales, reglamentarias y administrativas referentes al acceso a la actividad de las entidades de crédito y su ejercicio* (COM(1998) 461 final).

⁵³ Como bien afirma HICKS, J., en *Ensayos críticos sobre la teoría monetaria*, Editorial Ariel, Barcelona, 1967, "cuando se pregunta al estudiante qué es el dinero no hay más elección posible que la definición convencional. El dinero se define por sus funciones: es dinero cualquier cosa que se usa como dinero. El dinero es lo que hace de dinero, y las funciones del dinero son tres: ser unidad de cuenta, ser medio de pago y ser reserva de valor".

⁵⁴ Permanece en manos del público, constituido por monedas y billetes, circunscrito en la actualidad como medio de pago a la realización de pagos de escasa cuantía.

⁵⁵ Nos referimos al que hallamos en los depósitos bancarios consistente en apuntes contables archivados en los soportes magnéticos de un ordenador.

⁵⁶ Vid. MATEO HERNÁNDEZ, J. L., *El dinero electrónico en internet*, *op. cit.*, pág. 114.

aqué cumplirá idénticas funciones que éste y se acercará en mayor o menor medida a todas sus características deseables, destacando en este terreno la búsqueda de un punto especialmente relevante para la consideración de auténtico efectivo, y que no es otro que la consecución del anonimato como característica inherente a éste en los pagos tradicionales.⁵⁸

El uso del dinero efectivo electrónico ha surgido recientemente como una alternativa a los pagos realizados con tarjetas ya que muchos usuarios de Internet se abstienen de realizar sus compras con tarjetas por la facilidad de rastrear la compra, sus nombres, números de tarjetas, gustos, preferencias etc.. El dinero electrónico aporta un elemento adicional de seguridad, al no dejar rastros de la compra, ya que en principio es anónimo.

La Directiva sobre regulación de las entidades emisoras de dinero electrónico define el dinero electrónico como un valor monetario representado por un crédito

⁵⁷ Ciertamente no existe unanimidad, ni desde el punto de vista técnico ni jurídico, sobre la terminología a utilizar a la hora de hacer referencia a este sustituto del dinero electrónico del dinero efectivo y así, en ocasiones, se equiparan términos como dinero electrónico, *e-cash*, *network money* o dinero de red, monedero electrónico, o *digital coins*, entre otros.

⁵⁸ Numerosos autores definen dinero electrónico como cualquier modalidad de pago que utilice tecnologías electrónicas. Otros, distinguen entre dinero electrónico en sentido amplio y el dinero electrónico en sentido restringido. En este sentido, RICO CARRILLO, M., "El pago mediante dinero electrónico", CBL-Journal, Cyberbanking & Law, Issue January, 2003: "En la noción << dinero electrónico en sentido amplio >> se identifica con cualquier sistema de pago que requiera para su funcionamiento una tecnología electrónica, abarcando esta denominación, las tarjetas electrónicas, los títulos valores electrónicos (cheques y letras de cambio), las cartas de crédito electrónicas, el dinero efectivo electrónico así como cualquier otra forma de pago que implique la existencia de un medio electrónico para hacerse efectivo. En sentido restringido, la noción "dinero electrónico" alude al "dinero efectivo electrónico" o dinero digital (en atención a la tecnología actualmente utilizada), utilizándose esta expresión únicamente para referirse a las monedas y billetes electrónicos como sustitutos del dinero metálico o del papel moneda tradicionalmente conocido." Dicha autora define en forma general el dinero electrónico como "un instrumento basado en el funcionamiento de una TEF (Transferencia Electrónica de Fondos) que tiene por objeto facilitar el pago en operaciones generalmente concertadas a través de redes de comunicación pudiendo asumir distintas formas según la voluntad de las partes negociantes." "Decimos que se trata de operaciones generalmente concertadas a través de redes de comunicación pues hay algunos casos, como las tradicionales tarjetas, que aun cuando implican el uso de medios electrónicos pueden ser utilizadas en cualquier establecimiento físico independientemente de la existencia de una red de comunicación. De otra parte hablamos del elemento volitivo como requisito indispensable para el uso del dinero electrónico, en el entendido que su aceptación siempre estará supeditada a la voluntad de las partes ya que no puede obligarse a nadie a recibir ni a efectuar un pago distinto del dinero efectivo tradicional calificado como de curso legal en cada una de las legislaciones existentes; así como los cheques y las tarjetas tradicionales requieren para su aceptación la manifestación del concurso de voluntades entre el vendedor y el comprador -y en algunos casos hasta del emisor del medio de pago-, de igual manera sucede con el dinero electrónico en cualquiera de sus distintas modalidades."

exigible a su emisor, almacenado en un soporte electrónico, -por ejemplo, una tarjeta inteligente o el disco duro de un ordenador- aceptado como medio de pago por empresas distintas de la entidad emisora, generado como un sustituto electrónico de monedas y billetes con la finalidad de realizar pagos de escasa cuantía por medios electrónicos. La definición citada abarca tanto al dinero efectivo contenido en los monederos electrónicos como el dinero generado a través de un software.

La Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social sobre un Marco de actuación para la lucha contra el fraude y la falsificación de los medios de pago distintos del efectivo, se refiere a los “instrumentos electrónicos con valor almacenado” incluyendo en esta categoría las tarjetas prepagadas y dinero electrónico basado en un programa informático.

El Real Decreto 322/2008, de 29 de febrero, sobre el régimen jurídico de las entidades de dinero electrónico define, en su artículo 1, apartado 2º, dinero electrónico como “el valor monetario representado por un crédito exigible a su emisor: a) almacenado en un soporte electrónico; b) emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido; c) aceptado como medio de pago por empresas distintas del emisor”. Como vemos, la definición del Real Decreto se aparta de la Directiva europea en el sentido de que la misma lo concibe con la finalidad de realizar pagos de escasa cuantía por medios electrónicos, si bien, en la definición del Real Decreto no se hace referencia a la cuantía de los pagos, sin limitar el importe de los mismos.

De los textos legales citados podemos diferenciar claramente dos tipos de dinero efectivo electrónico, el dinero contenido en un dispositivo electrónico -una tarjeta-, en este caso nos referimos a los monederos electrónicos descritos anteriormente y el dinero efectivo generado a través de un programa de ordenador.

Para la generación del dinero efectivo electrónico a través de un programa de ordenador, es necesario, en primer lugar, tener una cuenta bancaria en una institución financiera⁵⁹ ya que son los fondos de esa cuenta los que permiten a su titular emitir dinero electrónico, en este sentido podemos decir que el dinero efectivo electrónico funciona de forma similar al cheque que es librado contra una disponibilidad de fondos.

⁵⁹ Las entidades de dinero electrónico se regulan en el citado Real Decreto 322/2008, de 29 de febrero, sobre el régimen jurídico de las entidades de dinero electrónico. Con independencia de las similitudes en el procedimiento de autorización de las EDE con otras entidades de crédito, en el real decreto se contemplan las especiales características de las EDE con un régimen diferenciado en un buen número de aspectos. Por un lado se establecen menores requisitos relacionados con la supervisión cautelar, como

Con el software apropiado se puede transferir dinero de la propia cuenta bancaria a través de Internet al disco duro del ordenador. En los billetes electrónicos, el papel moneda se sustituye por un conjunto de bits representativos de un determinado valor denominados *tokens*, que se almacenan en ficheros del disco duro del ordenador y que pueden transferirse a través de la Red a cambio de un producto o servicio. Para tener validez, los tokens deben ser similares al dinero metálico o de papel, así como en los billetes y monedas tradicionales el banco se compromete a su reconocimiento por un valor determinado, de la misma manera los billetes y monedas electrónicas deben estar respaldados por un determinado valor, tratándose en este caso de un valor prepagado, siendo la institución financiera la encargada de autenticar su emisión. Por otra parte deben reunir las mismas características de identificación de sus homólogos en papel: 1) estar identificados con un número de serie único, 2) contener el valor nominal, 3) estar fechados y 4) firmados por la entidad emisora. Para certificar su valor, el banco emisor firma los tokens con su firma digital y carga en la cuenta del usuario la cantidad de dinero real correspondiente al dinero digital generado.

Uno de los principales problemas que se presentan con el uso de este sistema es la facilidad de copiar el billete emitido electrónicamente y la posibilidad de cobrar el mismo billete más de una vez. Estos problemas se solucionan en principio, con la ayuda de técnicas criptográficas en la generación del dinero electrónico y con un control exhaustivo de parte de la institución financiera que respalda la emisión del dinero electrónico.

Uno de los sistemas de dinero efectivo existente en la actualidad es el denominado *E-Cash* gestionado por la empresa *Digi-Cash*, consistente en la emisión de unos pequeños archivos que equivalen a dinero digital. Para usar el *E-Cash* tanto el comprador como el vendedor necesitan tener abierta una cuenta en uno de los bancos que emiten el dinero electrónico⁶⁰, siendo la propia institución financiera la que facilita el software de emisión del dinero efectivo electrónico.

En el momento de generar el billete, el usuario le asigna un valor nominal y un número de serie (el software está programado para generar números de serie aleatorios suficientemente largos para evitar la duplicidad en la generación de los

un capital mínimo inferior o la no sujeción a determinados preceptos de la normativa bancaria, mientras que, por otro, se limitan las actividades que tales entidades pueden llevar a cabo y se impone un régimen de inversiones obligatorias en determinados activos.

⁶⁰ Deutsche Bank, en Alemania, Swiss NetPay AG en Suiza, St. George Bank en Australia y el Bank Austria en Austria son los principales bancos en el mundo que emiten *E-Cash*.

billetes), lo firma y lo envía a la institución financiera quien luego de verificar el número de la cuenta del usuario y la disponibilidad de fondos, procede a firmar el billete con una clave, certificando el valor nominal solicitado, y se lo envía al usuario. Una vez que el usuario ha recibido el billete firmado por el banco, lo puede almacenar en una billetera electrónica o lo puede usar inmediatamente para pagar sus compras en los establecimientos adheridos al sistema. El comerciante, al recibir el billete, lo envía a la entidad emisora y ésta, una vez que ha comprobado la autenticidad de la moneda, acredita el valor del billete en la cuenta del comerciante. Para evitar que el billete sea cobrado dos veces, el banco emisor debe contar con una base de datos que le permita verificar los números de serie de los billetes que han sido pagados.

El problema que se presenta con este procedimiento es que no garantiza en forma absoluta el anonimato del billete pues el banco siempre sabrá la serie de billete que ha firmado y a quién se lo ha firmado, pudiendo conocer, gracias a estos datos, cuándo, cómo y dónde fue gastado el billete. Para solucionar esta situación se ha ideado el sistema de la “firma digital a ciegas”, mediante el cual el usuario, antes de enviar la moneda para que la firme el banco, multiplica el número de serie por un factor conocido como “factor ciego” con la finalidad de ocultar el verdadero número de serie del billete electrónico, siendo imposible relacionar el número de serie del billete con el número obtenido después de aplicar el factor ya que sólo el usuario conoce el factor. Cuando el usuario recibe el billete divide el número firmado por el banco aplicando el mismo coeficiente que utilizó para generarlo, obteniendo el número de serie oculto, de manera que es imposible conocer quien ha gastado el billete ya que el banco cuando firmó el billete sólo sabía que se trataba de un billete de un determinado valor solicitado por uno de sus clientes⁶¹.

En la actualidad las entidades autorizadas⁶² para la emisión y gestión del dinero electrónico se agrupan en dos categorías: entidades de crédito y las entidades de dinero electrónico propiamente dichas.

La Directiva 2000/12/CE, que regula en forma general el funcionamiento de las entidades de crédito, las habilita para emitir y gestionar medios de pago, incluyendo dentro de estos medios, la emisión del dinero electrónico⁶³.

⁶¹ Sobre el funcionamiento del dinero efectivo electrónico vid. ÁLVAREZ MARAÑÓN, G., “Dinero electrónico”, en *PC World*, noviembre, 1999, págs. 332-333 y DÁVILA MURO, J., MORANT RAMÓN, J.L. y SANCHO RODRIGUEZ, J., “Dinero digital: pagos sin rastro”, ICADE, 1995, pp. 107-119.

⁶² De acuerdo con lo establecido en la Directiva 2000/46/CE.

De acuerdo con los principios establecidos en el artículo 1 de la Directiva 2000/46/CE, una entidad de dinero electrónico es una empresa o cualquier otra persona jurídica, distinta de una entidad de crédito, que emite medios de pago en forma de dinero electrónico.

El artículo 1 del RD 322/2008 define a las EDE como “aquellas entidades de crédito distintas de las definidas en el artículo 1,1,a)⁶⁴ del Real Decreto Legislativo 1298/1986, de 28 de junio, sobre la adaptación del derecho vigente en materia de entidades de crédito al de las Comunidades Europeas, cuya actividad principal consista en emitir medios de pago en forma de dinero electrónico, en los términos previstos por el presente real decreto”

La Directiva 2000/46/CE regula las condiciones a que deben someterse las entidades que se dediquen a la emisión del dinero electrónico, estableciendo una serie de requisitos relacionados principalmente con el monto mínimo del capital inicial⁶⁵, el mantenimiento de fondos propios permanentes⁶⁶ y la limitación de sus participaciones en empresas, actividades comerciales e inversiones, siendo sujetas a la verificación del cumplimiento de estos requisitos por parte de las autoridades competentes.

Con el objeto de fomentar la confianza en el uso del dinero generado a través de medios electrónicos, la Directiva establece y regula el derecho del portador de solicitar el reembolso del dinero electrónico a su valor nominal, en monedas y billetes de banco o por transferencia a una cuenta, sin otros gastos que aquéllos que resulten estrictamente necesarios para ejecutar la operación.

Según todo lo expuesto, por dinero electrónico⁶⁷ ha de entenderse un valor monetario representado por un crédito exigible a su emisor, almacenado en un soporte electrónico, emitido al recibir fondos de un importe cuyo valor no será inferior al valor monetario emitido y aceptado como medio de pago por empresas distintas del emisor. Para poder proceder a la emisión de dinero electrónico son

⁶³ Vid. Anexo I de la Directiva.

⁶⁴ “1. A efectos de la presente disposición, y de acuerdo con la Directiva 2000/12/CE del Parlamento Europeo y del Consejo, de 20 de marzo de 2000, relativa al acceso a la actividad de las entidades de crédito y a su ejercicio, se entiende por “entidad de crédito”: a) Toda empresa que tenga como actividad típica y habitual recibir fondos del público en forma de depósito, préstamo, cesión temporal de activos financieros u otras análogas que lleven aparejada la obligación de su restitución, aplicándolos por cuenta propia a la concesión de créditos u operaciones de análoga naturaleza.”

⁶⁵ No inferior a un millón de euros. Dicha obligación viene recogida en el Real Decreto 322/2008.

⁶⁶ 2% del importe de sus obligaciones financieras derivadas del dinero electrónico en circulación. De forma idéntica se recoge en el Real Decreto.

necesarios una serie de procedimientos de gestión y controles específicos, que garanticen su buen funcionamiento y la estabilidad del sistema financiero. En este sentido, corresponderá al Ministerio de Economía y Hacienda, previo informe del Banco de España, la autorización de la creación de Entidades de Dinero Electrónico y al Banco de España el control e inspección de las mismas así como su inscripción en el registro creado a estos efectos.

La Ley 44/2002, de Medidas de Reforma del Sistema Financiero, regula el dinero electrónico dentro del capítulo correspondiente a la “innovación tecnológica”. Mediante esta ley se transpone la Directiva 2000/46/CE, de 18 de septiembre, del Parlamento Europeo y del Consejo, sobre acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades⁶⁸. El dinero electrónico es, según la definición legal, un valor monetario representado por un crédito exigible a su emisor, almacenado en un soporte electrónico, emitido al recibir fondos de un importe no inferior al valor monetario del mismo y aceptado como medio de pago por empresas distintas del emisor⁶⁹.

Según CARRASCOSA, POZO ARRANZ y RODRÍGUEZ DE CASTRO⁷⁰, el dinero electrónico es “aquel instrumento de pago reflejado en un soporte informático, que a través de las transferencias electrónicas de fondos persigue la misma finalidad que el dinero tradicional, dependiendo de la efectividad del mismo de su realización”. Por lo cual, el dinero electrónico carece de eficacia liberatoria hasta su definitiva realización en papel-moneda por el estricto cumplimiento del artículo 1.170 del Código Civil.

En definitiva, podemos concluir que el dinero electrónico es una representación en soporte informático del dinero tradicional, que puede cumplir alguna de sus

⁶⁷ Partiendo de la base de que se está pensando en pagos de cuantía limitada, entendiéndose con arreglo al artículo 1.3,b).

⁶⁸ Esta Directiva viene a llenar una laguna legislativa en cuanto a la emisión del dinero electrónico o dinero red.

⁶⁹ Según la Directiva, el dinero electrónico ha de entenderse como una forma digital de efectivo, es decir, de papel-moneda. Y, a diferencia de la transferencia electrónica de fondos, en la que interviene un tercero (banco o entidad) en su efectiva realización, el dinero electrónico no necesita de la autorización ni la participación de persona o entidad alguna; en definitiva, es “un substitutivo electrónico de las monedas y los billetes de banco, almacenado en un soporte electrónico como, por ejemplo, una tarjeta inteligente o una memoria de ordenador y que, en general, está pensado para efectuar pagos electrónicos de poca monta”.

⁷⁰ CARRASCOSA LÓPEZ, V., POZO ARRANZ, M. Y RODRÍGUEZ DE CASTRO, E. P., *La contratación informática: el nuevo horizonte contractual*, Granada, Comares, 1997, pág. 34.

funciones, pero que en realidad no es dinero en sentido estricto, ya que carece de alguno de los requisitos, como por ejemplo la aceptación universal o el carácter obligatorio de medio de pago. El problema es que la referencia legal española y la normativa comunitaria son muy amplias. También la precisión del concepto desde el punto de vista jurídico y económico presenta dificultades. Incluso, últimamente se está diferenciando entre dinero electrónico en sentido amplio y dinero en Red⁷¹.

El dinero, en definitiva, no es otra cosa que la representación de un valor abstracto, admitido para la realización de intercambios y respaldado por una autoridad pública. En el supuesto del dinero electrónico esta representación, en lugar de papel, estaría contenida en bits y, concretamente, en cupones criptográficos. Tal como señala MARTÍNEZ NADAL⁷², “con el dinero electrónico se intenta ofrecer las mismas ventajas que con el dinero físico, que son básicamente las siguientes: a) Aceptación universal como medio de pago. b) Pago garantizado que no depende de la existencia de fondos en una cuenta ni la concesión de crédito de un tercero. c) Inexistencia de costes para el usuario. d) Anonimato: No queda ni rastro de las personas que lo utilizan (problema asociado a los protocolos de pago mediante tarjeta, pues al entregar el número de tarjeta en cada compra se deja un rastro fácil de seguir que permite construir un perfil del titular)”⁷³.

Una de las principales inquietudes que manifiestan los usuarios de Internet a la hora de efectuar un pago con dinero electrónico se relaciona directamente con su incertidumbre acerca de la admisión legal del pago efectuado a través de estos nuevos medios.

Podemos declarar la admisibilidad legal del pago con dinero efectivo electrónico basándonos en las siguientes premisas:

⁷¹ En este sentido VEGA VEGA, J. A., *Contratación electrónica y protección de los consumidores*, cit., pág. 321.

⁷² MARTÍNEZ NADAL, A., *Medios de pago en el comercio electrónico*, Actualidad Informática, Aranzadi, Octubre, 2000, pág. 9.

⁷³ Probablemente, la más conocida de las propuestas sobre dinero electrónico sea la aportada por la corporación norteamericana Ecash Technologies [<http://www.ecashtechnologies.com/>], cuya iniciativa de pago ha conseguido ciertas dosis de popularidad en los Estados Unidos. Veamos, muy brevemente, cómo funciona. En principio, su funcionamiento podría estructurarse en dos fases: 1º Creación del dinero electrónico: Para poder utilizar esta forma de pago, el usuario debe convertirse en titular de una cuenta corriente en una entidad bancaria que emita moneda electrónica. Previa petición del cliente al banco, el usuario, mediante un software suministrado por la entidad, puede crear y gestionar una cuenta de dinero

1. La autonomía de la voluntad y la libertad de pacto: según estos principios de carácter general, el pago por medios electrónicos será válido siempre que las partes hayan convenido en ello. En el caso de un pago distinto al dinero efectivo tradicional siempre se requerirá un pacto de esta naturaleza, en virtud de que no puede obligarse al acreedor a aceptar un medio de pago distinto del dinero efectivo.

2. La validez del contrato electrónico: hoy en día, la mayoría de las legislaciones admiten la validez del contrato efectuado por medios electrónicos. Siendo el pago un medio de ejecución del contrato, en este caso un medio electrónico de

electrónico en la que tendrá la facultad de «crear» tanto «*e-money*» como dinero tenga en su cuenta real. Al «crear» dinero electrónico, el software gestor de su cuenta atribuye a cada «*cybermoneda*» un número de serie aleatorio que es firmado digitalmente por el usuario y enviado al banco para que éste atribuya a la nueva «*cybermoneda*» un valor económico determinado (Si el titular atribuye un número a las «*cybermonedas*» y luego las remite al banco para que las firme y atribuya un valor monetario, la entidad bancaria podrá conocer, registrando el número de las «*cybermonedas*», quien realiza el pago mediante la confrontación de éstos con las «*cybermonedas*» remitidas por los comerciantes. Para evitarlo se empleó una técnica conocida como firma ciega. Antes de enviar las «*cybermonedas*» con su número aleatorio y firmadas por el titular, este número aleatorio se multiplica por un número determinado (conocido como factor ciego), mutando el número real de las «*cybermonedas*» y firmándolas el titular en este momento. De esta forma, el banco nunca sabrá el número real de las *cybermonedas*, pudiendo el titular preservar su anonimato en sus compras electrónicas). Recibido por el banco, éste procede a verificar la firma digital y a comprobar la identidad del cliente y la integridad del mensaje. Realizado esto, el banco firma digitalmente la «*cybermoneda*» atribuyéndole un valor económico determinado, valor que, simultáneamente, es descontado de la cuenta tradicional del titular. Finalmente, el titular recibe la moneda firmada por el banco con un valor determinado, preparada para ser usada como medio de pago en el ámbito del comercio electrónico (el titular recibe las «*cybermonedas*» con el valor monetario asignado por el banco y procede a obtener el número real de las mismas. Para ello divide el número por el factor ciego, obteniendo el número serie original de la «*cybermoneda*», número que jamás será conocido por el banco porque el número que remitió y firmó fue otro, garantizándose así el anonimato en el pago).

2º Pago mediante dinero electrónico: Llegado el momento del pago, el titular, mediante el software de gestión, transferirá al comerciante «*cybermonedas*» por el importe de la deuda. Recibidas por el comerciante, éste conecta con el banco y verifica dos extremos: a) La autenticidad de éstas, comprobación que realiza la entidad bancaria verificando su firma electrónica en las «*cybermonedas*» remitidas por el comerciante. b) Las «*cybermonedas*» no han sido usadas. Realizadas estas comprobaciones, la entidad bancaria ingresa en la cuenta del comerciante la cantidad económica equivalente al valor de las monedas. A simple vista es fácil reconocer las ventajas que el *e-money* ofrece como modo de articulación del cumplimiento del pago: Pago anónimo, sencillo, seguro, universalmente admitido. No obstante, también presenta dificultades que no deben ser obviadas: El esfuerzo de las entidades bancarias que, con el fin evitar un doble uso de las mismas, deberán almacenar el número de serie de cada «*cybermoneda*» gastada, labor que con la generalización de su uso y con el transcurso del tiempo puede convertirse en una tarea ingestible o el propio coste en tiempo por la continua necesidad de conexión con el banco, tanto por parte del titular de las *cybermonedas* como del comerciante.

ejecución de un contrato electrónico, no vemos objeción alguna para declararlo legalmente admisible.

3. La representatividad del medio de pago: para validar el pago a través de signos representativos del dinero (letras de cambio y cheques), la mayoría de las legislaciones admiten el principio de que el pago puede hacerse en dinero efectivo o en un signo que lo represente, como ha quedado de manifiesto a lo largo de esta ponencia, el dinero electrónico no es más que una representación binaria del dinero tradicional, siendo en todo caso susceptible de conversión a dinero real en beneficio de los derechos del portador.

5.2. NATURALEZA JURÍDICA

Tal como hemos señalado más arriba, tenemos que partir de la idea de que el dinero electrónico en puridad no es dinero. No cumple la característica de servir de medio de pago con carácter general para la extinción de las obligaciones, ni es aceptado con carácter general en las transacciones económicas. Es una representación digitalizada del dinero. Sin embargo, el dinero electrónico opera en las transacciones económicas y puede servir para extinguir obligaciones, por lo que nos surge la duda acerca de su concepción y naturaleza jurídica⁷⁴.

La Ley 22/2002, sobre ordenación económica, en su artículo 21 y el Real Decreto 322/2008 en el artículo 1, lo describen como “un valor monetario”. Al tratarse de una representación de un derecho en soporte informático o electrónico y que puede ser negociado, es claro que se trata de un valor. Avanzando en este análisis, algún sector doctrinal se cuestiona el hecho de si estaríamos en presencia de un título valor. Dado que no participa de la naturaleza tradicional de los títulos valores, ni en esencia ni por requisitos, no podemos calificarlo de título valor. En todo caso, podría hablarse de un título valor digital o, en su caso, virtual. Esta categoría no está plenamente consolidada ni definida en la dogmática jurídica, por lo que sería difícil aceptarla por ahora. Además, a primera vista nos

⁷⁴ Para un estudio más específico de la naturaleza jurídica y un contraste de pareceres, puede verse GUARRACINO, F., “Titolo di credito elettronico e documento informatico e documento informatico”, en *BBTC*, núm. 4, julio-agosto de 2001, pp. 525 y ss.; OLIVIERI, G., “Appunti sulla moneta elettronica”, en *BBTC*, Núm. 6, noviembre-diciembre 2001, pp. 810 y ss.; PASTORSEMPERE, M.C., *El dinero electrónico*, Ed. de Derecho Reunidas, Madrid, 2003, pp. 247-310; RICO CARRILLO, M., “Dinero electrónico”, en *RCE*, núm. 31, octubre 2002, pp. 2 y ss.; SANTAELLALÓPEZ, M., “Las telecomunicaciones y los medios de pago electrónicos”, en *ICDE*, núm. 43, enero-abril, 1998, pp. 95 y ss.

encontramos con inconvenientes que por ahora se nos antojan infranqueables, pues aunque incorpora un derecho a un documento (digital), no se cumplen otros principios o requisitos de los títulos valores. En primer lugar, la autonomía para el ejercicio de los derechos es cuestionable. Por otra parte, en cuanto al principio de legitimación, tenemos que admitir que en el momento de la transacción no sabremos si esa instrumentalización de dinero electrónico es válida, ya que depende de la certificación bancaria para saber si es posible el ejercicio del derecho que supuestamente confiere. A falta de precisión, la concepción de valor monetario, si no suficiente, al menos sirve para delimitar su naturaleza jurídica y diferenciarlo de otros instrumentos que pueden cumplir funciones análogas pero que tienen connotaciones propias⁷⁵.

Configurada su esencia, nos fijaremos en sus características para precisar mejor su naturaleza jurídica. El dinero electrónico tiene como características principales las siguientes: a) *representación digital*: el dinero electrónico se representa por medios electrónicos, de ahí que el medio de transmisión sean las múltiples anotaciones electrónicas, que equivalen al desplazamiento posesorio, que produce la transferencia del valor representado; b) *versatilidad*: en una economía globalizada el dinero puede facilitar los distintos pagos que deban hacerse en el ámbito internacional, ya que puede estar expresado en cualquier moneda y los emisores pueden “acuñar” dinero en la moneda demandada por un operador económico o consumidor para realizar sus pagos; c) *anonimato*: el sistema utilizado por el dinero electrónico preserva el anonimato del consumidor, pero no del receptor del dinero (prestador del servicio o vendedor), ya que éste debe conectarse con el banco para hacer efectivo el dinero electrónico percibido. Por lo tanto, una de las mayores preocupaciones de los Gobiernos, el uso de dinero en efectivo para blanqueo y pago de operaciones ilegales, queda automáticamente resuelto, ya que, aunque no se puede rastrear la identidad del pagador, sí se conoce la identidad del que recibe el dinero, invalidando por tanto la posibilidad de usar dinero electrónico para financiaciones ilegales; d) *no aceptación obligatoria*: el dinero electrónico no es de curso legal, por lo que su utilización con poder liberatorio solo tendrá lugar en el supuesto de que el acreedor lo acepte; en la actualidad no existe obligación, de ahí que la evolución en el uso dependerá de la regulación legal; en estos momentos no es un medio de pago universal⁷⁶.

⁷⁵ Véase sobre el particular VEGA VEGA, J. A., *Contratación electrónica y protección de los consumidores*, cit., pp. 321-323, que alude a esta cuestión y al que, en esencia, seguimos.

⁷⁶ VEGA VEGA, J. A., *op. cit.*, pág. 323.