La Economía Digital: El dinero electrónico y el lavado de dinero

MAURICIO DEVOTO

CENIT. Centro de Investigaciones de Tecnologías de la Información de Buenos Aires. Argentina

INTRODUCCIÓN

La aproximación a nuevas realidades y conceptos como el DINERO ELECTRÓNICO requiere indispensablemente el conocimiento del marco o contexto general que les sirve de base y facilita su desarrollo. No podemos desconocer que nos encontramos ante nuevas manifestaciones y nuevos contenidos que surgen en una "NUEVA ECONOMÍA". Esta nueva economía nos obliga a adaptarnos rápidamente a los cambios introducidos por las nuevas tecnologías, sin dejar de reconocer que la recepción de la tecnología de la información con los alcances que vemos hoy en día, y que produce impactos en la economía, el comercio, la educación, las telecomunicaciones, la privacidad y el derecho, requiere un cambio cultural muy importante.[1]

La utilización del vocablo "TECNOLOGÍA" se repite incesantemente.

■[1] LYNCH, Horacio M., NOTAS SOBRE EL DERECHO EN LA ERA DIGITAL, La Ley, 15 de mayo de 19 96.

Definimos a la tecnología como el conjunto de conocimientos científicos, técnicos y artesanales que permiten producir un bien o servicio. Generalmente se habla de "NUEVAS TECNOLOGÍAS". Se dice que son nuevas porque nacen después de la Segunda Guerra Mundial, y desde entonces se han desarrollado ininterrumpidamente. Se pueden agrupar dichas tecnologías en tres grandes grupos: las tecnologías de la información, las biotecnologías y las tecnologías de los nuevos materiales.[2]

Estas palabras mágicas se presentan cualquiera sea el ámbito en el que nos encontremos: cuando leemos un artículo sobre medicina, cuando nos enteramos que un diario se edita simultáneamente en varias ciudades en tiempo real, cuando nuestro amigo agricultor nos comenta acerca de las bondades de las semillas que acaba de sembrar. Por otro lado, miramos rápidamente las noticias que tratan sobre el mundo de la telefonía, las fusiones de empresas, la guerra de las tarifas, los servicios integrados, etc., y observamos indiferentemente como operarios que pertenecen a empresas de cable instalan cables por encima de nuestras cabezas a los que llaman fibra óptica, mientras otros que pertenecen a las compañías telefónicas hacen otro tanto por debajo de nuestros pies. Y nos preguntamos que habrá detrás de todo ello.

Podemos entonces hacer una primera distinción, relacionando el ámbito en el que se desenvuelve el tema que nos ocupa con el grupo de tecnologías que corresponden a dicho ámbito. Desde este punto de vista, analizaremos el "dinero electrónico" como una de las aplicaciones derivadas del desarrollo de la tecnología de la información (Information Technology) en la nueva economía digital.

Toda transferencia electrónica de valores implica una transmisión de mensajes. Un tema clave en la transmisión de información, y fundamentalmente en redes abiertas, es el de la seguridad. Al respecto, veremos los principios básicos de la Criptografía y estudiaremos una de sus aplicaciones más difundidas en la actualidad: la firma digital.

Seguridad y privacidad parecen ser los requisitos indispensables para el desarrollo y aceptación de los nuevos sistemas de pago en la economía digital. En muchos casos la premisa es el anonimato. Analizaremos, por último, la relación

[2] FERRARO, Ricardo A., EDUCADOS PARA COMPETIR, Ed Sudamericana, 1995.

existente entre las ventajas ofrecidas por estos nuevos mecanismos de pago y el lavado de dinero.

1. LA ECONOMÍA DIGITAL

1.1 Nueva Economía. Antigua Economía.

La NUEVA ECONOMÍA, la ECONOMÍA DIGITAL, surge principalmente de la convergencia de distintas culturas que trabajaban y se desarrollaban en forma independiente. Por un lado la industria de la computación (computadoras, software y servicios), las comunicaciones (telefonía, cable, satélite) y los contenidos (entretenimientos, editoriales y proveedores de información). Esta convergencia ha dado lugar a la nueva industria multimedia.[3]

Una de las características fundamentales de esta nueva economía es la "DIGITALIZACIÓN". La digitalización implica que la información, ya se trate de imagen, texto o sonido, se convierte al lenguaje de las computadoras: los números binarios. La información se reduce a ceros y unos, y se diferencia según la forma en la que estos ceros y unos se agrupen. A modo de ejemplo podemos tomar el caso de un disco de pasta y un disco digital (CD). En los primeros, la información se graba físicamente en el surco dando lugar a depresiones y picos. Mediante la utilización de una púa, se amplifican las alteraciones contenidas en los surcos dando lugar al sonido que escuchamos. Con el transcurso del tiempo, las depresiones y picos se van erosionando (ralladuras, grasitud, desgaste de la púa, polvo), lo que produce una disminución en la calidad del sonido. En el disco digital, en cambio, al realizarse la grabación, la información se convierte en ceros y unos, descomponiéndose en pequeñísimos fragmentos. Para escuchar lo grabado necesitamos un aparato que vuelva a unir aquello que se encuentra desfragmentado en el disco. Por lo tanto, el sonido que escuchamos no es el mismo ejecutado en el acto de la grabación, sino que se compone de la unión de todos aquellos fragmentos. La perfección y rapidez del sistema hace que creamos que estamos escuchando un sonido continuo, cuando en realidad no lo es.

En la ANTIGUA ECONOMÍA la información era análoga. La gente se comunicaba moviendo su presencia física hacia una sala de reuniones, hablando a

[3] TAPSCOTT, Don. THE DIGITAL ECONOMY, Mc. Graw Hill, 1995.

través de una línea telefónica análoga, enviando cartas, yendo al banco a realizar depósitos o extracciones, sintonizando señales análogas de televisión, exhibiendo fotografías reveladas en negocios especializados, intercambiando dinero efectivo o cheques, publicando revistas que se adquirían en un negocio o se distribuían por correo, o proyectaba luz a través de una tira de un film en un cine o teatro.

En la NUEVA ECONOMÍA la información se presenta en forma digital: en bits.

Cuando la información se digitaliza y se comunica a través de redes digitales, aparece un nuevo mundo de posibilidades. El proceso de digitalización permite reducir la cantidad de información a transmitir, y la información puede ser comprimida. A esto se le suma el desarrollo del medio físico por donde transita la información, encontrándonos con la fibra óptica en lugar del típico cable de cobre o par trenzado, que permite transmitir mayor cantidad de información (ancho de banda) a la velocidad de la luz. Por otro lado, la digitalización permite la combinación de diversos tipos de información, por ejemplo en documentos multimedia. La información puede ser almacenada y recuperada instantáneamente desde cualquier lugar del mundo.

1.2 La Autopista de la Información

La autopista de la información es el elemento que sirve de sustento a esta nueva economía digital. La autopista deriva de la convergencia de los contenidos informacionales, los diferentes medios de comunicación y las nuevas tecnologías de la información. Es una infraestructura física basada en la utilización de cables, teléfonos o satélites sobre los que se desenvuelven los sistemas informáticos distribuidos en redes locales, nacionales o internacionales. Internet, como la conocemos en la actualidad, debe ser considerada como el inicio de una infraestructura mundial de información, que recibe indistintamente diversas denominaciones: Autopista de la Información (Information Superhighway, I-Way), Infraestructura Nacional de Información (National Information Infraestructure, NII), o Infraestructura Global de Información (Global Information Infraestructure, GII). Constituye un vasta red de más de cinco millones de nodos informáticos y más de 60 millones de usuarios.

En la autopista de la información, las distancias ya no son importantes, pero la posibilidad de acceso a la misma, la confidencialidad, la seguridad y la identificación de los participantes adquieren cada vez mayor valor, dado que los

mismos se esfuerzan por preservar su intimidad, individualidad y propiedad. En el espacio virtual, la identidad de las personas que transitan por la autopista de la información revestirá una importancia sin igual. La desmaterialización de las transacciones aumenta el riesgo de que una persona transite con una identidad ficticia o usurpe la identidad de otra persona. De esta manera la problemática relacionada con el desarrollo de la autopista de la información, y más específicamente, del comercio electrónico en un entorno abierto, radica en dos factores claramente indisociables: la seguridad técnica y la seguridad jurídica de las transacciones desmaterializadas.

La seguridad es uno de los temas centrales y claves en el desarrollo de toda infraestructura de información, ya sea a nivel nacional como global. Los participantes quiere tener la certeza de que la persona con la que están contratando es efectivamente quien dice ser, y que la información o mensajes transmitidos no han sufrido alteración durante su transmisión. La Criptografía, a través de la Firma Digital, aporta las soluciones que permiten garantizar el "no repudio" y la "inalterabilidad" del mensaje.

Pero además de estas inquietudes los participantes quieren confidencialidad, es decir, que la información solo pueda ser leída por el sujeto a quien va dirigida.[4] La tecnología, a través del encriptado de los mensajes, aporta la solución adecuada.

Volveremos más adelante sobre este tema.

Esta REVOLUCIÓN DIGITAL, que da lugar a la nueva economía, es fuente generadora de nuevos contenidos. Es decir que nos encontramos con un nuevo mundo en el que todo está por hacer, en el que la imaginación tendrá un papel fundamental.

El dinero electrónico consiste en un nuevo contenido, un nuevo producto surgido de la imaginación del hombre en el marco de la nueva economía digital.

■[4] CAVOUKIAN, Ann - TAPSCOTT, Don. WHO KNOWS. SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD, Mc. Graw Hill, 1997.

2. EL COMERCIO ELECTRÓNICO Y LOS MEDIOS DE PAGO

2.1 Comercio Tradicional y Comercio Electrónico

Uno de los mayores impactos de la Tecnología de la Información se verifica en el comercio y los servicios financieros.

El comercio electrónico ha modificado los hábitos de las finanzas y el de los comerciantes y consumidores, a la vez que produce cambios sustanciales en los medios de pago tradicionales.

El tema de la seguridad merece especial atención: es un elemento clave en este tipo de transacciones en tanto el medio por donde transita la información es, en principio, inseguro.

Las ideas desarrolladas en la nueva economía, que dan lugar a nuevos contenidos y nuevos productos, están poniendo en jaque la continuidad de la empresa tradicional, que debe adaptarse rápidamente a los cambios que se producen en la era digital. Miles de millones de dólares se encuentran en danza y a la espera de ser aprovechados por los que primero o de mejor manera sepan advertir y manejar la situación.

Por ejemplo, en el ámbito de los medios de pago, si los bancos asumen una fuerte intervención en los pagos realizados a través de Internet, como lo hacen en los pagos tradicionales, pueden ganar mucho dinero transfiriendo fondos y emitiendo credenciales a consumidores y comerciantes.

Por otro lado, si empresas de otro tipo advierten la lentitud con la que los bancos se mueven y organizan sus propios sistemas de pagos on line (en línea), serán ellas las que consigan los beneficios.

Según un estudio realizado por la firma KILLEN & ASSOCIATES[5] de California para MCI, en 1994 se realizaron transacciones en el mundo por U$S 4.6 trillones, de los cuales U$S 595 billones, aproximadamente el 13%, fueron

[5] ABA BANKING JOURNAL, Noviembre de 1995.

realizadas por catálogo, TV, EDI (Electronic Data Interchange), y redes on line, incluida Internet. Como van las cosas, se considera que todas las operaciones de este tipo tenderán a trasladarse a Internet en los próximos diez años.

El informe considera que en el año 2000 se realizarán compras de bienes y servicios vía Internet por U$S 600 billones, y por U$S 1,5 trillones en el 2005; en cuanto a cantidad de pagos, sostiene que en el año 2000 se realizarán U$S 7 billones por Internet, y U$S 17 billones en el 2005. Calculando un cargo (fee) de U$S 1,50 por transacción, las organizaciones que dominen el comercio por Internet se llevarán U$S 11 billones en el 2000 y U$S 26 billones en el 2005, contra un costo aproximado del 50 al 60% de dichas sumas.

Mientras todos estos sistemas diferentes se desarrollan y adquieren estructuras más complejas, la pregunta clave es quién se sentará en el lugar más alto del podio, las nuevas empresas o la industria de los bancos.[6]

El comercio electrónico en general, e Internet en especial, fueron ideados para el intercambio de información. Sin embargo, en la actualidad se los utiliza en gran medida para transacciones que requieren el posterior transporte de la mercadería objeto de la transacción. En este caso, Internet es una simple alternativa comparable al teléfono, que no agrega nada nuevo al comercio. La tecnología base del comercio electrónico es solamente una parte de las transacciones. La compra electrónica será la comercializadora inevitable de la Internet, pero los que la defienden fervorosamente deberían tener en cuenta que los hábitos de los consumidores son difíciles de romper, ya que generalmente les gusta elegir y tocar la mercadería.

■[6] Es interesante la lectura del artículo titulado EL FIN DE LOS BANCOS, publicado en la revista INFORMATION TECHNOLOGY, No.2, junio de 1996, del que destacamos: "La Revolución multimedia generará cuatro impactos en el sector bancario: Primero: Los Bancos pueden ser desplazados de su papel de proveedores de productos y servicios financieros, caer en un proceso de desintermediación. Segundo: El cambio tecnológico también impulsará la creación de nuevas formas de pago electrónico. Tercero: La banca electrónica no es aun un negocio redituable. Sin embargo los beneficios se percibirán en el largo plazo. La penetración a través de medios como Internet se dará donde no se requiera una ligazón con la infraestructura local. El verdadero peligro de la desintermediación se encuentra en la línea de productos, como la de inversión, que no necesita el sistema doméstico. Para no perder clientes, los bancos deberán ofrecer una amplia gama de servicios, pero cuentan con un arma estratégica LA MARCA. Cuarto: Donde esté la ventaja competitiva, estará el negocio. El sector basaba su estrategia en tener una gran cadena de distribución, muchos clientes y productos que fueran comoddities. Hoy los banqueros manejarán dos negocios distintos: sus productos y su marca".

Es razonable suponer que el comercio electrónico tendrá limitaciones evidentes si se lo compara con las formas tradicionales de compra de los consumidores actuales. Al realizar una compra de mercadería o servicios en general, intervienen distintos factores: educación, interacción social, suerte para encontrar ofertas y posibilidad de probar lo que se quiere comprar. La compra electrónica no puede duplicar fácilmente estas experiencias.

Si esto es así, conviene concentrarse en las excepciones, en aquellas situaciones en que no se necesita elegir o tocar la mercadería. Esto nos sugiere campos tales como: comercio sobre dinero (finanzas); comercio sobre títulos y commodities (bolsa) y, fundamentalmente, el comercio sobre información electrónica. Este último tendrá mucho futuro porque, en verdad, es el medio más apropiado para elegir, probar, sentir, enviar, y embalar los productos electrónicos.

La conclusión precedente indica que la verdadera promesa de Internet radica en la venta de información. El software, por ejemplo, que es en esencia pura información, es generalmente transferido a un medio físico (el disquete), empacado, transportado y vendido en negocios. Esta cadena encarece enormemente el costo de la información. Mucho más barato y eficiente es adquirir esa información vía Internet y recibirla directamente en el lugar, entorno y destino natural: la computadora del comprador.

En contraste con la simple mudanza a Internet del comercio tradicional, la venta de información sufrirá cambios importantes. Estos cambios producirán en el futuro nuevos problemas legales y sociales, o cuanto menos, acentuarán los ya existentes. Sin perjuicio que en la actualidad el acceso a la mayor parte de las páginas de la Web es gratuito y abierto a cualquiera que desee acceder a las mismas, esta situación puede cambiar cuando los pioneros del océano de la información comiencen a crear zonas económicas exclusivas y limiten el acceso a aquellos que hayan adquirido una clave de acceso o cuenten con motores de búsqueda configurados para realizar pagos por el acceso a páginas de la WWW. Las páginas de Web son ideales para la proliferación de las micro transacciones, en las que el lector deba pagar una pequeña cantidad (10 centavos o menos) por cada acceso. Este tipo de transacciones no resulta económicamente viable a través de sistemas de tarjetas de crédito, y tampoco parece que lo será en el futuro. En consecuencia, será necesario el desarrollo de un medio digital que permita la transferencia de valores, y, preferentemente, que no requiera la participación de terceros como el

emisor de las tarjetas, como paso previo a que los micro pagos se constituyan en parte de la nueva economía.[7]

2.2. Sistemas de Pago

Podemos intentar una clasificación distinguiendo entre tarjetas de crédito, los denominados cheques digitales y el Dinero Electrónico. Haremos una breve referencia a los dos primeros, dejando el estudio del dinero electrónico para un capítulo aparte.

2.2.1. Sistemas basados en Tarjetas de Crédito

En la actualidad las tarjetas de crédito y débito se erigen en el medio más simple, aunque no necesariamente ideal, de transferir valores a través de Internet. Estos sistemas pueden agruparse en tres categorías:

* El consumidor envía un e-mail al comerciante con los datos de su tarjeta o llena un formulario en una página de World Wide Web, de la misma forma que se envía la misma información a través del correo. Sin perjuicio que existe algún riesgo de que la información transmitida sea copiada durante la transmisión, existen muy pocos casos denunciados.

* El consumidor encripta los datos de su tarjeta de crédito antes de enviarlos, utilizando programas especialmente diseñados para tal fin, como por ejemplo PGP[8] o el protocolo "Secure Sockets Layer" que se encuentra incorporado al Netscape. La seguridad que proporciona esta tecnología torna casi imposible la interceptación de los datos por un intruso. MASTERCARD y VISA han adoptado una norma común para el comercio electrónico: SET, Secure Electronic Transaction.. Esta tecnología intenta superar cinco grandes desafíos: a) garantizar reserva en la información de pedidos y pagos., que se logra por la encriptación de los mensajes; b) asegurar la integridad de todos los datos transmitidos, a través de la firma digital; c) verificar que el titular de la tarjeta de crédito sea usuario legítimo de una cuenta, mediante la utilización de la firma

[7] FROOMKIN, Michael. LIVING WITH ANONYMITY, DIGITAL CASH, AND DISTRIBUTED DATABASES.

[8] PRETTY GOOD PRIVACY. En Internet: http://www.pgp.com/

digital y los comprobantes de comerciante; d) garantizar la autenticidad del comerciante para que pueda aceptar pagos con tarjetas bancarias a través de una institución financiera; y e) facilitar y alentar la interoperatividad entre proveedores de redes y de software.

(*) Para realizar la operación el consumidor utiliza el servicio de un tercero, al que le envía por otro medio (off line) los datos de la tarjeta de crédito.

a) Un ejemplo es THE FIRST VIRTUAL INTERNET PAYMENT SYSTEM (FV). Para asociarse, se necesita una dirección de e-mail, dado que toda comunicación entre el usuario y FV se realizará a través de ese medio, incluida la confirmación de la compra por parte del usuario y la autorización a FV para cargarla a su tarjeta de crédito. El sistema funciona aproximadamente de esta forma: Se accede a la página de FV, luego de llenar la aplicación se activa la cuenta enviando telefónicamente a FV los datos de la tarjeta. FV confirma la apertura enviando al solicitante un mensaje vía e-mail conteniendo el número de identificación (Virtual PIN) que deberá ser utilizado para operar el sistema . Para realizar una compra, el usuario da el V.PIN al vendedor, quien se comunica con FV indicándole que ha recibido la orden de realizar una operación con el mencionado número de identificación. FV envía al comprador un e-mail para que este confirme o cancele la operación o denuncie si hubo un fraude. El costo de tener un V.PIN es de U$S 2 por año.

b) En otros casos los consumidores pueden detentar un par de claves que les permiten firmar digitalmente los mensajes.

En ambos casos los comerciantes perfeccionan las transacciones comunicándose previamente con la tercera parte (FV o la autoridad certificante), antes que el precio sea cargado a la tarjeta del comprador.

2.2.2. Cheques Digitales

Este segundo sistema funciona como si se tratara de cheques reales, salvo que el usuario utiliza una firma digital para firmar el cheque y luego transmitirlo en línea (on line) encriptado. Como ejemplo de empresas proveedoras de este servicio se puede citar a CHECK FREE[9] y NETCHEQUE[10].

[9] En Internet: http://www.checkfree.com/

El usuario necesita una chequera electrónica, que actualmente consiste en una tarjeta del tamaño de una tarjeta de crédito que puede contener datos y se inserta en un slot que puede ser incorporado en la mayoría de las computadoras portátiles que se ofrecen en el mercado. En el futuro la chequera se llevará en una tarjeta inteligente (smart card), que cuenta con un chip y distintos tipos de memoria, que le permitirá generar cheques, llevar su registro de cheques y guardar claves públicas y privadas. Los pequeños comerciantes necesitarán una tarjeta de PC (PC card), mientras que los demás comerciantes tendrán que incluir un procesador especial en sus servidores. Los mensajes transmitidos entre clientes, comerciantes y bancos contarán con la seguridad y confidencialidad que brinda la criptografía de clave pública y la firma digital, que más adelante analizaremos.

Las encuestas realizadas informan que sigue siendo importante el hecho de que el dinero no se ha debitado inmediatamente de las cuentas corrientes. Actualmente los débitos se realizan entre las 24 y 36 horas.

3. EL DINERO ELECTRÓNICO

3.1. Definición

El término dinero electrónico es utilizado en forma general para hacer referencia a una amplia gama de mecanismos de pago utilizados en el comercio electrónico. Al hablar de dinero electrónico debemos mentalizarnos en que trataremos con productos ofrecidos por empresas. Estos productos almacenan valores, es decir, registran los fondos o valores disponibles por un usuario del sistema, en un aparato o dispositivo electrónico que se encuentra en su poder.

Dichos valores son adquiridos por el consumidor, al igual que se adquieren otros instrumentos prepagos como los travellers cheques, y se reducen en la medida que son utilizados para realizar compras. A diferencia de muchos otros esquemas de prepagos basados en tarjetas, que se utilizan para un único propósito como los ofrecidos por las compañías telefónicas, los productos de dinero electrónico tienden a ser diseñados como un medio de pago general.

■[10] En Internet: http://nii-server.isi.edu/info/NetCheque/

El dinero electrónico, así definido, se diferencia de los llamados "access products", o productos de acceso, que permiten al consumidor utilizar medios electrónicos para acceder a otros servicios convencionales de pago, por ejemplo la utilización de una PC y de una red como podría ser Internet para realizar un pago con tarjeta de crédito o para transmitir instrucciones tendientes a la realización de una transferencia de fondos entre bancos.

En la actualidad no se ha adoptado formalmente, a nivel internacional, una terminología determinada respecto del dinero electrónico. Los sistemas de pago que utilizan tecnologías como ser tarjetas inteligentes (smart cards) o Internet, utilizan diferentes denominaciones: "E-Money", "digital cash", "cybermoney", "cybercurrency" y "cyberpayments". Muchas veces un mismo término puede tener sentidos diferentes según el contexto y las circunstancias en el que se lo utilice.

3.2. Sistemas

Sin perjuicio de lo expresado podemos identificar tres tipos de sistemas de dinero electrónico:[11]

Sistemas implementados con un soporte en tarjeta (card-based).

Estos sistemas proveen al consumidor una tarjeta inteligente o smart card. La tarjeta trae incorporado un chip que contiene un sistema operativo y aplicaciones de software, que son insertados en la tarjeta en el proceso de su manufactura. La emisión de las tarjetas a los consumidores se realiza de diferentes formas: en algunos casos, la tarjeta involucra una cuenta bancaria perteneciente al usuario; alternativamente, las tarjetas puede ser adquiridas anónimamente en máquinas expendedoras o mediante la utilización de tarjetas de crédito o débito. La institución emisora u operadora central del sistema provee a los comerciantes de terminales u otros dispositivos que permiten realizar la operación. La carga de los valores en las tarjetas se realiza generalmente a través de un cajero automático (ATM - Automatic Teller Machine) o de un teléfono equipado especialmente. En general, y como expresamos anteriormente, de estas transacciones resulta un débito en la cuenta bancaria preexistente del consumidor que está ligada a la tarjeta. Para realizar una compra el usuario introduce su tarjeta en la terminal del

[11] V. AN INTRODUCTION TO ELECTRONIC MONEY ISSUES, trabajo preparado por personal del Departamento del Tesoro de los Estados Unidos para la conferencia "Toward Electronic Money and Banking: The Role of Government", Washington DC, septiembre de 1996.

vendedor e ingresa la suma a pagar. La terminal verifica que el balance que surge de la tarjeta permita realizar la transacción e instruye para que debite la suma correspondiente al pago. Luego la tarjeta instruye a la terminal del vendedor para que incremente su balance en la misma suma.[12]

Sistemas basados en un software especial (software-based). Estos sistemas funcionan por medio de un programa instalado en la computadora del usuario. Están diseñados para realizar pagos a través de redes, fundamentalmente Internet. El proceso de carga se realiza por el intercambio de mensajes entre los dispositivos del usuario y del emisor, mensajes que son trasmitidos por la red. En la práctica, se tiende a involucrar -por razones de seguridad- la emisión de documentos o cheques firmados digitalmente. El proceso de pago depende del diseño del producto de que se trate, así como del contexto en el que el pago se realiza. La determinación de la cantidad y características de las entidades emisoras, cuyas obligaciones son electrónicamente transmitidas en un sistema de dinero electrónico, son críticas desde un punto de vista financiero, y afectan asimismo la implementación técnica de dicho sistema. Los sistemas que se basan en un solo emisor pueden no necesitar un clearing de las transacciones realizadas, siempre y cuando otra institución no participe colectando o distribuyendo fondos. En sistemas con múltiples emisores, el número de tarjeta o un certificado emitido por una autoridad certificante dentro de una infraestructura de firma digital, identifica al usuario, y las transacciones comerciales y demás operaciones son trasmitidas al ente emisor para su registro. Este registro puede servir tanto para fines de clearing financiero como para brindar seguridad al sistema.

Sistemas híbridos, que utilizan tecnologías que permiten utilizar las tarjetas inteligentes en conexión con sistemas basados en redes.

■[12] SECURITY OF ELECTRONIC MONEY, Report by the Committee on Payment and Settlement and the Group of Computer Experts of the central banks of the Group of Ten countries, Basle, agosto de 1996.

3.3. Principales Características del Dinero Electrónico

Como mencionarámos más arriba, nos encontramos frente a productos comerciales[13]. Mientras que el objetivo de todas las empresas es facilitar y darle mayor eficiencia a las transacciones, reforzar y sostener el poder adquisitivo en Internet, y por supuesto, obtener un beneficio, los productos ofrecidos presentan distintas características. Sin perjuicio de ello, y a efectos de este trabajo, se debe reconocer que salvo un producto en particular, todos los demás tienen un punto en común: la ausencia del anonimato. Entre ellos podemos nombrar a CYBERCASH[14] y MONDEX.[15]

La excepción a esta regla general es DIGICASH.[16] DIGICASH es una empresa radicada en Amsterdam y creada David Chaum, reconocido experto en criptografía. El aporte de Digicash al comercio electrónico es un producto denominado ECASH. ECASH está diseñado para realizar pagos seguros entre computadoras, ya sea por email o Internet. Sin entrar en mayores detalles técnicos, es necesario aclarar que para proveer seguridad y privacidad, DIGICASH utiliza la firma digital con una característica distintiva: la firma es "ciega" (blind signature). Esto hace que ecash, no pueda ser rastreado. El ocultamiento (blinding) realizado por el dispositivo o computadora del usuario hace que nadie pueda relacionar el pago con quien lo realiza. Sin perjuicio de ello, el usuario puede probar inequívocamente haber realizado o nó un pago determinado, sin tener que revelar más información.

Dejando de lado que en el futuro los sistemas de pago analizados difieran en cuanto a sus alcances en las particularidades enunciadas, se pueden observar ciertas características distintivas entre los sistemas de pago existentes y los sistemas

■[13] BORTNER, Mark. CYBERLAUNDERING: ANONYMOUS DIGITAL CASH AND MONEY LAUNDERING. En Internet:
http://www.law.miami.edu/¬froomkin/seminar/papers/bortner.htm

■[14] En Internet: http://www.cybercash.com/

■[15] En Internet: http:www.co.uk/mondex.html

■[16] En Internet: http://www.digicash.com/

de dinero electrónico, independientemente que asimismo existen diferencias entre los propios sistemas de moneda digital.[17]

4. INFRAESTRUCTURA DE SEGURIDAD

4.1 Introducción. Seguridad, Privacidad y Anonimato.

Como indicáramos al comienzo, la seguridad es uno de los temas fundamentales de los que dependerá el futuro de la autopista de la información, y en especial, el futuro del comercio electrónico y los mecanismos de pago que dependen de la transmisión de información en redes abiertas. Puede decirse entonces que para que el comercio electrónico pueda continuar desarrollándose y se consolide definitivamente es necesaria la implementación de una infraestructura adecuada que le permita sobreponerse a su peor enemigo: la inseguridad propia del medio por el que transita la información.

Se sostiene que el desarrollo de la infraestructura de información depende de la iniciativa privada. En materia de seguridad, en cambio, las afirmaciones no son tan concluyentes. Las consecuencias que deriven de la infraestructura de seguridad adoptada, que pueden salir de la órbita de los particulares para tocar puntos relacionados con la seguridad nacional, ameritan un análisis más profundo.

En el caso de empresas que desarrollen productos que requieran la transmisión de información, es lógico suponer que tratarán de incorporar aquellos mecanismos que brinden al usuario la mayor seguridad posible, de forma tal que este pueda tener certeza en cuanto a la identidad de la persona con la que se está comunicando, que la información transmitida o recibida no ha sufrido alteraciones durante la transmisión, y que nadie salvo el destinatario tiene acceso a la información transmitida.

La presencia o ausencia de estas bondades determinará la mayor o menor aceptación de los mismos por parte de los usuarios.

En ciertos productos la seguridad y privacidad alcanzan su cenit con el anonimato -recordar el dicho popular: "EN INTERNET NADIE SABE QUE ERES UN PERRO"-. La tecnología utilizada no solo garantiza la seguridad de la

[17] FinCEN. CYBERPAYMENTS: AN INTRODUCTORY SURVEY, 1995

información transmitida o recibida por el usuario, sino que asimismo permite ocultar su identidad, o al menos, su identificación con una operación determinada.

Analizado el tema desde otro punto de vista, la seguridad, la confidencialidad y el anonimato, llevados a su máxima expresión, alentarían la utilización de estos productos con fines ilícitos.

Esta contradicción ha dado lugar a duros enfrentamientos entre los defensores a ultranza de la privacidad y los gobiernos y organismos encargados de ejecutar las leyes.[18]

4.2 Inseguridad del medio - Criptografía[19]

Las características de los sistemas de redes abiertas, como Internet, han determinado que el medio en el cual se transmite la información en el comercio electrónico sea inseguro.

Aunque no está al alcance de cualquier persona, un operador experimentado puede interceptar la información. Por ello se han desarrollado distintos mecanismos para proteger la información que se transmite. Hasta el momento, lo más efectivo ha sido recurrir al cifrado de la información.

Esto nos introduce en la ciencia de la Criptografía, que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, utilizada tradicionalmente en los ámbitos militar, diplomático y comercial[20].

■18 V. THE CENTER FOR DEMOCRACY AND TECHNOLOGY. En Internet: http://www.cdt.org/

■19 V. DEVOTO, Mauricio - LYNCH, Horacio M. BANCA, COMERCIO, MONEDA ELECTRÓNICA Y LA FIRMA DIGITAL, La Ley, 21 de marzo de 1997.

■20 Existen muchos trabajos sobre este tema. Recomendamos la lectura de "RSA FAQ ON CRYPTOGRAPHY" (1995), en Internet: http://www. rsa.com/ rsalabs/newfaq/

4.2.1 Criptografía con clave secreta

La criptografía tradicional se basa en el concepto de que tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave secreta. El que envía el mensaje utiliza una clave secreta para encriptarlo y el que lo recibe utiliza la misma clave para desencriptarlo. Este método se conoce como Criptografía con Clave Secreta. El principal problema consiste en conseguir que ambas partes conozcan la misma clave sin que ningún tercero se entere. Si la clave es interceptada, quien la conozca podrá luego utilizarla para leer todos los mensajes encriptados.

La Criptografía con clave secreta ha tenido dificultades para brindar la seguridad necesaria en este aspecto.

4.2.2 Criptografía con clave pública

Existe un acuerdo generalizado acerca de que el sistema que mayor seguridad brinda en la actualidad a las transacciones electrónicas e intercambio electrónicos de datos, es el de la Criptografía de Clave Pública, basado en algoritmos asimétricos. Fue desarrollada en 1976 en la Universidad de Standford, Estados Unidos, con el propósito de resolver el problema de la administración de claves[21]. En este sistema cada persona obtiene un par de claves, llamadas clave pública y clave privada. Cada usuario debe generar su propio par de claves, por intermedio de un software confiable. La clave pública de cada persona se publica y la privada se mantiene en secreto. La necesidad de un remitente y un receptor de compartir la misma clave queda eliminada. Ya no es necesario confiar en los canales de comunicación, corriendo el riesgo de que alguien esté escuchando en la línea telefónica o de que se viole el secreto de la clave privada. Cualquier persona puede enviar un mensaje confidencial con sólo utilizar la clave pública, pues el mensaje solamente puede desencriptarse con la clave privada que posee el receptor únicamente.

Por este medio, se obtienen transacciones seguras y auténticas, con la certeza de la integridad de los datos y la imposibilidad de repudio por parte del emisor. Pero para poder cumplir con estos principios, la Criptografía de Clave

[21] La producción, transmisión y almacenamiento de las claves se denomina administración de claves. Actualmente, se ha ampliado a otros usos mucho más próximos aunque con niveles de exigencia diferentes.

Pública debe basarse en una adecuada infraestructura de manejo de claves y productos adecuados, que permita identificar en forma indubitada a particulares y corporaciones con sus claves públicas, a través de terceras partes confiables (las Autoridades Certificantes).

El sistema requiere una infraestructura grande y compleja, pero esencial: sin ella los usuarios no podrán saber con quién están tratando en la red, a quién le están enviando dinero, quién firmó un documento, o si la información fue interceptada y alterada durante la transmisión.

Por ello los usuarios demandarán una fuerte infraestructura de administración o manejo de claves basada en autoridades certificantes que operen bajo estrictas normas predeterminadas.

La determinación de la referida estructura está relacionada con la política de intervención legislativa que se adopte con referencia a la validez del documento electrónico[22], Este tema si bien se vincula íntimamente con el objeto del presente estudio, será analizado en otro trabajo, limitándonos aquí a enunciar las posturas generalmente adoptadas.[23]

Se han advertido entonces distintas posturas legislativas respecto de la validez del documento electrónico: a) una postura amplia en que el legislador establece la validez del documento electrónico, sin hacer referencia a su soporte material ni al tipo de lenguaje a utilizar. Tampoco se analiza o se ajustan otras normas que hacen referencia al documento tradicional (es el caso del Proyecto del Estado de California, y de la Electronic Signature Act of 1996, del Estado de Florida); b) una postura restringida en que el legislador se preocupa no sólo de establecer la validez jurídica del documento electrónico sino también de reglamentar su uso, a la vez que determina detalladamente la infraestructura técnica y operacional que se utilizará para la inserción del mismo en la práctica comercial (como enUtah Digital Signature Act, de 1995; y Georgia Digital Signature Act de 1996); c) una postura detallista en que el legislador revisa todo el cuerpo legal para derogar, modificar o agregar normas que hagan compatibles el sistema con el

■22 En los Estados Unidos existen pocos casos judiciales que se refieran a la validez de la firma digital en los contratos. Para más detalles, ver artículo sobre ELECTRONIC SIGNATURES, NEW YORK LAW JOURNAL, el 30 de octubre de 1995

■23 V. MICCOLI, Silvia. LA SICUREZZA GIURIDICA NEL COMMERCIO ELETTRONICO, TESI DE LAUREA, UNIVERSITA' DEGLI STUDI DI PISA, FACOLTÀ DI GIURISPRUDENZA".

documento electrónico (como en el caso del Proyecto del Gobierno de Alemania); y por último, d) algunas combinaciones, donde se encuentra un sistema de intervención junto con algunas características de las posturas antes referidas. (como en el Proyecto de Ley sobre Documento Electrónico realizado por Ediforum Italia y Proyecto de Ley sobre Documentos Electrónicos de Chile[24]).

4.3 Infraestructura: Monopolio de la Criptografía por parte de la National Security Agency (NSA)

Existen en los Estados Unidos restricciones impuestas por el gobierno al desarrollo y difusión de las tecnologías criptográficas. La NATIONAL SECURITY AGENCY (NSA) fue creada por orden del Presidente Truman en 1952, siendo su función primordial la intervención en el área de comunicaciones, interceptando y descifrando las comunicaciones secretas de otros gobiernos.

La NSA tiene la posibilidad de interceptar la mayor parte -sino todos- los mensajes electrónicos que entran, transitan o salen de los Estados Unidos. En los 45 años transcurridos desde su creación, la NSA ha gozado del monopolio virtual del área de la tecnología criptográfica. Argumentando que su misión requiere que dicha tecnología sea celosamente protegida, la agencia ha procurado mantener su monopolio y suprimir toda iniciativa privada no gubernamental que tuviera por objeto el desarrollo y difusión de la criptografía. Se considera que la motivación existente detrás de los esfuerzos para limitar el know how es evidente: a medida que aumenten y se difundan los conocimientos para lograr mayor seguridad en el encriptado de información, mayores serán las dificultades y el tiempo que la agencia necesitará para desarrollar su propio trabajo.

Los esfuerzos de la NSA para mantener su monopolio se han extendido al área de las exportaciones y política comercial. La exportación de software que contenga elementos de criptografía es regida por el INTERNATIONAL TRAFFIC IN ARMS REGULATION (ITAR). Mientras la Agencia niega los cargos, los representantes de la industria claman que las restricciones impuestas por la NSA frenan la innovación en un área fundamental para la industria de la computación, a la vez que provocan que las compañías americanas pierdan mercados en manos de competidores de otros países.

4.4 Infraestructura: Gobierno e Industria. Necesidad de trabajo conjunto

[24] Proyecto realizado por el ESTUDIO JARA, DEL FAVERO & COMPAÑÍA.

Se sostiene en los Estados Unidos que el Gobierno y la industria deben trabajar conjuntamente a efectos de crear una infraestructura que brinde seguridad y permita el desarrollo de productos que incorporen elementos de criptografía, sin menoscabar la seguridad nacional y pública. Una política que considere claves criptográficas como base para acuerdos gubernamentales bilaterales y multilaterales sería determinante para que la industria pueda desarrollar productos que operen mundialmente. La industria participará en la definición de algoritmos y protocolos estándar, y desarrollará productos de claves de encriptado adecuados para la protección de los sectores de información públicos y privados. El Gobierno colaborará estableciendo estándares para la INFRAESTRUCTURA DE ADMINISTRACIÓN DE CLAVES (IAC) y proveerá un mercado para productos de seguridad.

Una infraestructura de Administración de Claves y adecuados productos de claves brindarán muchos beneficios, tanto local como internacionalmente, mientras se consideran las ventajas de la red global para un comercio mejorado, más ágil y seguro.

Como se dijo antes, se insiste en que el gobierno no puede seguir con el monopolio de la criptografía. Ya no resulta aceptable el argumento de que la única información que merece interés de seguridad nacional es la información gubernamental. Por otro lado, resulta irreal creer que el gobierno brindará soluciones acordes a la velocidad con que se suceden los cambios en INFORMATION TECHNOLOGY. Poco a poco, todas las instituciones, ya sean civiles o militares, y las corporaciones, se van comunicando a través de conexiones comunes. El comercio nacional e internacional se está mudando a la red[25].

Existe otro argumento de peso que obliga al gobierno a ser socio en el desarrollo de la infraestructura antes referida. No sólo la Era de la Información produce cambios radicales en la forma en que la gente interactúa, sino que la dependencia de los sistemas de información hace a las instituciones vulnerables en un grado antes inimaginable. Casi todas las instituciones de las que la seguridad pública depende se encuentran ante graves riesgos debido a su presencia y dependencia dentro de una infraestructura de información global.

■[25] V. entre otros a FROOMKIN, Michael, "THE METAPHOR IS THE KEY: CRYPTOGRAPHY, THE CLIPPER CHIP, AND THE CONSTITUTION"; SCHMID, Dan, NOTES FOR SECURITY AND ENCRYTION ON THE NET; DORNEY, Maureen S., THE GRIP ON ENCRYPTION, en Internet: http:// www. ipmag.com/dorney.html.

Pero la proliferación de servicios criptográficos no está exenta de riesgos. Las claves pueden perderse, ser robadas u olvidadas, tornando inútiles los datos encriptados. Adicionalmente, la utilización indiscriminada del encriptado sin características que brinden la adecuada seguridad pueden poner en un serio peligro a la sociedad.

5. FIRMA DIGITAL - LA LEY DEL ESTADO DE UTAH

En los Estados Unidos varios estados están desarrollando o han implementado una legislación sobre firma digital, entre ellos Arizona, Georgia[26], Hawai, Oregon, Washington[27], Illinois, California[28] y Florida[29].

La mayoría de esta legislación se ha basado en la Ley del Estado de Utah sobre la Firma Digital[30] (UTAH DIGITAL SIGNATURE ACT), que comenzó a regir el 1 de mayo de 1995, y en la Guía de Firma Digital[31] (DIGITAL SIGNATURE GUIDELINES), publicada en octubre de 1995 por THE AMERICAN BAR ASSOCIATION'S INFORMATION SECURITY COMMITTEE (Comité de la ABA SCIENCE AND TECHNOLOGY SECTION)[32].

Utah fue el primer estado en haber implementado un nuevo uso en la autopista informática. Ante la ausencia de una ley modelo, la Ley de Firma Digital de Utah se ha convertido en referencia obligada para los demás estados.

■[26] En Internet: http://www.cc.emory.edu/ BUSINESS/ digital_signature _draft.html

■[27] En Internet: http://access.wa.net/sb6423_info/6423.html

■[28] En Internet: http://www.gcwf.com/articles\digsig.htm

■[29] En Internet: http://www.complaw.com/pgp/digsiglegis.html

■[30] En Internet: http://www.gov.state.tu.us/ccjj/digsig/

■[31] En Internet: http://www.gov.state.tu.us/ccjj/digsig/dsut-gl.html

■[32] Ver asimismo el artículo publicado por ZANGER, Larry, COMPUTER LAW COMMITTEE OF THE CHICAGO BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES WITH MODEL LEGISLATION, en Internet: http:// www.imginfo.com/caug/ ca_1195a.thm

Esta ley conforma un esquema regulatorio que brinda efectos legales a la firma digital, un sistema de doble clave que brinda protección, verificación y autenticación a transacciones en línea (on-line).

En el acto electrónico interviene un tercera parte que es la autoridad certificante, encargada de emitir los certificados indispensables para poder utilizar el sistema, cuyas funciones describiremos más adelante.

5.1. Firma y verificación

La Ley define la firma digital ("dig-sig") como la transformación de un mensaje empleando un criptosistema asimétrico tal que una persona que posea el mensaje inicial y la clave pública del firmante pueda determinar con certeza:

si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y ii] si el mensaje ha sido modificado desde que se efectuó la transformación. Esta definición es importante ya que decide la tecnología a utilizar, que recae fundamentalmente en la criptografía, cuya definición y características hemos brindado anteriormente.

La firma digital utiliza un criptosistema asimétrico. Esto significa que comprende dos procesos: i] la creación de la firma por el suscriptor utilizando la clave privada, que es sólo conocida por el suscriptor, y el es el único responsable de su guarda, y ii] la verificación de la firma por la otra parte: el receptor del mensaje comprueba su autenticidad utilizando la clave pública que surge del certificado del suscriptor, comunicándose con el repositorio o registro donde el referido certificado se encuentra registrado.

Una típica transacción con firma digital comienza con la determinación por parte del firmante del contenido del documento que desea firmar (mensaje plano). Luego el software crea una imagen digital o resumen del mensaje mediante la aplicación de una función denominada "hash function". Al resultado de la aplicación de esta función se lo denomina "hash result", y consiste en un código único para el mensaje. De esta forma, si el mensaje cambia o es modificado, el "hash result" será diferente. Por último el software encripta o transforma el "hash result" con la firma digital mediante la aplicación de la clave privada del firmante. La firma así obtenida es única tanto para el mensaje como para la clave privada utilizada para su creación.

La verificación de la firma digital es realizada computando un nuevo "hash result" del mensaje original utilizando la misma "hash function" usada en la creación de la firma digital. Finalmente, con la clave pública que surge del certificado del firmante, el receptor comprueba si la firma digital proviene del la clave privada del firmante y si el nuevo "hash result" es igual al que proviene de la firma digital. El receptor realiza esta operatoria comunicándose con el registro de claves públicas donde se encuentra registrado el certificado correspondiente.

5.2 Terceras partes confiables: Autoridades Certificantes

La infraestructura o el sistema requiere de terceras partes confiables.

La ley de Utah le da una importancia fundamental a las Autoridades Certificantes (CERTIFICATION AUTHORITIES, "CAS"), definidas como las personas facultadas para emitir certificados[33] Pueden ser personas físicas o empresas o instituciones públicas o privadas y deberán obtener una licencia de la DIVISION OF CORPORATIONS AND COMMERCIAL CODE, en el caso del Estado de Utah, para funcionar como tales.

Son las encargadas de mantener los registros directamente en línea (on-line) de claves públicas. Una compañía puede emitir certificados a sus empleados, una universidad a sus estudiantes, una ciudad a sus ciudadanos.

Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser confiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que atestigüe la validez de su clave. Esta solución da origen a diferentes niveles, estratos o jerarquías de CAs.

5.2.1 Certificados

Los Certificados son registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad. Permiten la verificación de que una clave pública dada pertenece fehacientemente a una determinada persona. Los certificados ayudan a evitar que alguien utilice una clave falsa haciéndose pasar por otro. En su forma más simple, contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número

[33] Respecto de la importancia de actuación de las autoridades certificantes, ver FROOMKIN, Michael, THE ESSENTIAL ROLE OF TRUSTED THIRD PARTIES IN ELECTRONIC COMMERCE, en http://www.law.miami.edu/-froomkin/articles/trusted1.htm

de serie del certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un

Registro (repository), considerado como una base de datos a la que el público puede acceder directamente en línea (on-line) para conocer acerca de la validez de los mismos. Los usuarios o firmantes (subscribers) son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante.

La Autoridad Certificante puede emitir distintos tipos de certificados. Los certificados de identificación simplemente identifican y conectan un nombre a una clave pública. Los certificados de autorización, en cambio, proveen otro tipo de información correspondiente al usuario, como dirección comercial, antecedentes, catálogos de productos, etc. Otros certificados colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para la atestación de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido. Otros certificados permiten determinar día y hora en que el documento fue digitalmente firmado (Digital time-stamp certificates).

El interesado en operar dentro del esquema establecido por la ley, luego de crear el par de claves deberá presentarse ante la autoridad certificante (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad y/o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita 'firmar' el documento de que se trate.

Por ejemplo, para realizar una operación financiera de importancia con un banco, éste puede requerir al interesado un certificado del que surja, además de la constatación de su identidad, el análisis de sus antecedentes criminales o financieros. Esto quiere decir que la firma digital del interesado sólo será aceptada por la otra parte si cuenta con el certificado apropiado para la operación a realizar.

5.2.2 Registro (Repository)

Como dijimos anteriormente, es la base de datos a la que el público puede acceder on-line para conocer acerca de la validez de los certificados, su vigencia o cualquier otra situación que se relacione con los mismos. Dicha base de datos debe

incluir, entre otras cosas, los certificados publicados en el repositorio, las notificaciones de certificados suspendidos o revocados publicadas por las autoridades certificantes acreditadas, los archivos de autoridades certificantes autorizadas y todo otro requisito exigido por la División. Para ser reconocido, el repositorio debe operar bajo la dirección de una autoridad certificante acreditada.

5.2.3 Un caso concreto. VeriSign[34]

VERISIGN es una de las empresas que brinda servicios de certificación. Estos servicios han sido diseñados básicamente para brindar seguridad al comercio electrónico y a la utilización de la firma digital. Para el logro de este objetivo, las autoridades de emisión (ISSUING AUTHORITIES, "IA") autorizadas por VERISIGN funcionan como trusted third partie, emitiendo, administrando, suspendiendo o revocando certificados de acuerdo con la práctica pública de la empresa. Las IA facilitan la confirmación de la relación existente entre una clave pública y una persona o nombre determinado. Dicha confirmación es representada por un certificado: un mensaje firmado digitalmente y emitido por una IA. El management del proceso de certificación incluye servicios de registro, "naming", autenticación, emisión, revocación y suspensión de los certificados.

Esta empresa ofrece tres niveles de servicios de certificación. Cada nivel o clase de certificados provee servicios específicos en cuanto a funcionalidad y seguridad. Los interesados eligen entre estos grupos de servicios el que más le conviene según sus necesidades, debiendo especificar qué clase de certificado desean. Dependiendo de la clase de certificado requerido, los interesados pueden solicitarlos y obtenerlos electrónicamente siguiendo las instrucciones detalladamente indicadas, o deberán concurrir personalmente a una LOCAL REGISTRATION AUTHORITY (LRA), o a un delegado, que puede ser un notario. Pueden existir varias "IA" para cada uno de los distintos niveles. Cumplidos los requisitos exigidos se emite el certificado o se envía un borrador para su aceptación por el interesado, según el caso.

Los Certificados Clase 1 son emitidos y comunicados electrónicamente a personas físicas, y relacionan en forma indubitable el nombre del usuario o su "alias" y su dirección de E-mail con el registro llevado por VeriSign. No autentican la identidad del usuario. Son utilizados fundamentalmente para Web Browsing y E-

[34] En Internet: http://www.verisign.com

mail, afianzando la seguridad de sus entornos. En general, no son utilizados para uso comercial, donde se exige la prueba de identidad de las partes.

Los Certificados Clase 2 son emitidos a personas físicas, y confirman la veracidad de la información aportada en el acto de presentar la aplicación y que ella no difiere de la que surge de alguna base de datos de usuarios reconocida. Es utilizado para comunicaciones intra-inter organizaciones vía E-mail; transacciones comerciales de bajo riesgo; validación de software y suscripciones on line. Luego del acuerdo del usuario, realizado on line ante una LRA, los datos contenidos en la aplicación son confirmados comparándolos con una base de datos reconocida. Teniendo en cuenta dicha confirmación la LRA puede aprobar o rechazar la aplicación. En caso de aprobación, la conformación es enviada por correo. Debido a las limitaciones de las referidas bases de datos, esta clase de certificados está reservada a residentes en los Estados Unidos y Canadá.

Los Certificados Clase 3 son emitidos a personas físicas y organizaciones públicas y privadas. En el primer caso, asegura la identidad del suscriptor, requiriendo su presencia física ante una LRA o un notario. En el caso de organizaciones asegura la existencia y nombre mediante el cotejo de los registros denunciados con los contenidos en bases de datos independientes. Son utilizados para determinadas aplicaciones de comercio electrónico como 'electronic banking' y ELECTRONIC DATA INTERCHANGE (EDI).

Como las IAs. autorizadas por VERISIGN firman digitalmente los certificados que emiten, la empresa asegura a los usuarios que la clave privada utilizada no está comprometida, valiéndose para ello de productos de hardware. Asimismo, recomiendan que las claves privadas de los usuarios sean encriptadas vía software o conservadas en un medio físico (smart cards o PC cards).

6. EL DINERO ELECTRÓNICO Y EL LAVADO DE DINERO

6.1. Generalidades

Expuestas las características generales de los sistemas de dinero electrónico y los mecanismos que se utilizan para garantizar la seguridad y privacidad de toda transmisión electrónica de mensajes, analizaremos su relación con el lavado de dinero.

Para ello recurriremos a las 40 Recomendaciones establecidas por FATF (Financial Action Task Force). Este Grupo de Acción Financiera sobre Lavado de Dinero fue convocado por el Grupo de los Siete (G-7) en la Cumbre Económica de París de 1989, con la misión de desarrollar y promover políticas de prevención y represión del lavado de dinero, y reúne a 26 países y dos organizaciones internacionales (Comisión Europea y Consejo de Cooperación de los Estados del Golfo Pérsico).[35]

Con relación al tema que nos ocupa, se establece que los países deben prestar especial atención a la amenaza que representa el desarrollo de nuevas tecnologías que favorecen el anonimato, tomando las medidas necesarias para prevenir la utilización de las mismas en el lavado de dinero (R.13).

En este sentido se promueve, a nivel internacional, el acercamiento de los organismos encargados del control del lavado de dinero con las empresas que desarrollan los productos de dinero electrónico.

El lavado de dinero se produce luego de la comisión de un delito, de donde surgen fondos que necesitan ser lavados. La detección de esta actividad ilicíta constituye la primera dificultad, sobre todo por el hecho de que los medios utilizados para el lavado no solamente son legales sino que constituyen actividades corrientes, como la apertura de cuentas en bancos, la adquisición de instrumentos monetarios y la transferencia electrónica de fondos.

Del exámen de las características anteriormente mencionadas surge claramente que el dinero electrónico tendría la particularidad de facilitar a los lavadores el ocultamiento del orígen de los fondos, permitiendo su anónima movilización. Es lógico suponer que si estos nuevos sistemas se desarrollan de forma tal que se acomoden a las necesidades de los lavadores mejor que los sistemas de pago existentes, seguramente van a ser utilizados.

6.2. Las 40 Recomendaciones y la dificultad de su aplicación.

1. Desintermediación. Cambio de rol de los intermediarios tradicionales.

[35] FATF VII. ANNEX TO THE PUBLIC FATF REPORT ON TYPOLOGIES, Febrero de 1997.

Una de las características distintivas de la economía digital es la desintermediación, es decir, la eliminación de todo aquello que se interpone entre las partes.

La presencia de esta característica se observa claramente en el desarrollo de los sistemas de dinero electrónico. Históricamente los controles han descansado en la intermediación de los bancos y otras instituciones financieras, que actúan como aduanas que los fondos generalmente deben atravesar y donde se deben mantener registros de las operaciones. De hecho, la mayor parte de la regulación contra el lavado de dinero, así como las 40 Recomendaciones de la FATF, están destinadas específicamente a las entidades financieras para que implementen medidas que aseguren la existencia de informes por escrito que permitan el seguimiento de las operaciones.

Como hemos visto, algunos sistemas de dinero electrónico facilitan el cambio de valores sin la participación de los bancos, lo que da por tierra con la ayuda anteriormente mencionada.

Con relación a este tema, se promueve la aplicación de todas las recomendaciones a instituciones financieras no bancarias (R.8). Por otro lado, se aconseja a los países miembros a que establezcan aquellas actividades realizadas por el sector no financiero que pueden resultar vulnerables al lavado de dinero, y en este caso, que impongan controles efectivos (R.9).

Teniendo en cuenta lo expresado, los servicios de dinero electrónico pueden resultar comprendidos dentro de estas recomendaciones.

2. El rol de las entidades encargadas de regular.

Se recomienda que los organismos de control aseguren que las instituciones supervisadas posean programas adecuados para prevenir el lavado de dinero. Con tal motivo, las autoridades competentes deben trazar pautas que ayuden a las instituciones financieras a dictar patrones sospechosos en las conductas de sus clientes (R. 26 a 29). Otro punto importante es que alguno de estos sistemas pueden ser ofrecidos por entidades que actualmente no están sujetas a regulación.[36]

■[36] V. LYNCH, Horacio M. BANCA Y MONEDA ELECTRÓNICA SEGÚN EL DEPARTAMENTO DEL TESORO, Rev. Información Empresaria, Diciembre de 1996.

3. Dificultad de cumplir algunas de las políticas recomendadas.

* Conozca su cliente

Los sistemas de dinero electrónico hacen muy difícil que se cumpla con el principio "conozca su cliente". En Internet, cuyas características principales analizamos anteriormente, un gran conglomerado internacional podría no distinguirse de un pequeño negocio que realiza sus primeras armas en el comercio.

* Registro de operaciones

Las recomendaciones requieren que las instituciones financieras mantengan determinados registros de las transacciones realizadas así como la verificación y registro de la identidad de los clientes y la autenticación de la estructura legal de sus negocios (R.10 y R.12). La forma en que los sistemas de dinero electrónico puedan implementar estas medidas resulta incierta.

* Identificación de actividades sospechosas

Se requiere que las instituciones financieras identifiquen y reporten cualquier actividad sospechosa, y desarrollen e implementen programas contra el lavado de dinero (R 14).

* Transmisibilidad

La mayor o menor facilidad para trasladar los valores, así como la necesidad de recurrir a la intervención del emisor o de un tercero a efectos de concretar la operación determinará el éxito de los sistemas. Algunos sistemas solo permiten la transferencia de valores entre un individuo, por un lado, y un comerciantes y el emisor del sistema, por el otro. Otros, en cambio, permiten la transferencia de valores entre individuos. Estos últimos serían el sistema ideal ya que el producto en más parecido al efectivo.

A efectos de controlar el flujo de valores se han propuesto distintas medidas, entre las que se destacan:

-Limitar las transacciones entre individuos a operaciones de poco monto. La tecnología permite que se almacenen montos ilimitados. Los emisores seguramente limitarán estos valores para reducir el peligro de fraudes, pero en

definitiva esto dependerá y será determinado por factores comerciales y de mercado.

-Limitar la utilización de valores a un tiempo o plazo determinado. Hay que tener en cuenta que los lavadores explotarán cualquier tipo de limitación que se establezca, como lo hacen en la actualidad, obteniendo múltiples tarjetas, utilizando diferentes nombres y distintos emisores.

-Aumentar el nivel de registro de operaciones:

Registro de transacciones: Se considera casi imposible el seguimiento de todas las transacciones. Incluso si la tecnología lo permitiera sería prohibitivo a nivel costos y generaría una enorme cantidad de datos que no tendrían valor ni utilidad. Además no sería aceptado por los consumidores que buscan privacidad.

Registro de Propiedad. Algunos sistemas ofrecerán tarjetas por ATM. Otros requerirán la apertura de una cuenta. Lógicamente el sistemas con menor control será el más atractivo.

4. Equilibrio entre la privacidad de los particulares, la seguridad pública y el acceso legal legítimo.

La velocidad, la seguridad y el anonimato de los sistemas de dinero electrónico constituyen características positivas que inducen a su utilización, pero a su vez, las mismas características resultan atractivas para ser utilizadas con propósitos ilícitos.

En este sentido, y recordando lo expresado al hablar del futuro de la protección criptográfica, se recomienda que la legislación sobre seguridad y secreto debe ser concebida de forma tal de no impedir medidas contra el lavado de dinero (R.2).

6.3. Eficacia de las técnicas tradicionales de investigación

Las técnicas tradicionales de investigación han sido diseñadas en virtud de ciertos supuestos:

* Bancos que realizan ciertas transacciones;

* La habilidad de las instituciones financieras para monitorear la actividad de los clientes;
* La utilización de dinero efectivo basado en papel.

El dinero electrónico no solo desafiará estos presupuestos sino la manera en que dichas investigaciones son conducidas.

¿Cuáles son esos desafíos que introducirá el dinero electrónico?

1. Menor vulnerabilidad en la detección de las operaciones. El transporte físico del efectivo siempre ha presentado problemas al lavador de dinero. Hasta resulta común el abandono de dinero por no poder ser transportado rápidamente.

El dinero electrónico reduce la necesidad del contrabando físico, permitiendo que en lugar de un envío repartido en valijas con doble fondo, grandes cantidades puedan ser transmitidas instantáneamente y en forma segura con unas pocas instrucciones. El dinero podría ser transportado a cualquier lugar del mundo sin la necesidad de pasar por el control de las instituciones intermediarias tradicionales.

En tal sentido se recomienda a los países estudiar la posibilidad de aplicar medidas para detectar o controlar los movimientos de efectivo y título negociables al portador a través de las fronteras nacionales.

2. La velocidad de las transacciones dificulta su control. La velocidad del movimiento del dinero electrónico, fundamentalmente a través de Internet, dificultará la tarea de los encargados de ejecutar las leyes en identificar o rastrear la transferencia de fondos. Estos sistemas de pago, combinados con la desintermediación a que hemos hecho referencia, dificultarán de igual manera la determinación de programas para prevenir el lavado de dinero.

3. Dificultad para detectar los fondos ilícitos dentro del volumen general de los negocios. En la actualidad se considera que solo una pequeña parte de los U$S 2 trillones que por día se transfieren electrónicamente en todo el mundo, corresponden a fondos ilícitos. Una vez que los sistemas de dinero electrónico se utilicen en larga escala, los mismos tomarán parte de la proporción de dichos fondos ilícitos, resultando difícil identificarlos dentro del volumen total.

El volumen y la velocidad del procesamiento computarizado de datos dificultarán el desarrollo de indicadores que permitan detectar actividades

sospechosas. Para tener una idea de los números que se manejan, el informe nos recomienda tener en cuenta las estadísticas que surgen de SWIFT (Society for Worldwide Interbank Financial Telecommunication S.C.), y compararlas con los números que se prevén para Internet:

SWIFT	
Fondos transmitidos electrónicamente por día:	U$S 2 trillones
Mensajes recibidos por día:	2,5 millones
por año:	580 millones
Transacciones por segundo	1.000
Países miembros	135
Usuarios	5.300
INTERNET	
Servidores	12,8 millones
Usuarios	62 millones
E-mail por mes	1 billón

Estos número sirven para demostrar como los números de SWIFT se verán opacados y como el control será aun mas difícil en el mundo del dinero electrónico.

La Recomendaciones 23 y 30 sugieren que los países consideren el registro de los flujos internos e internacionales de dinero en efectivo, en cualquier moneda, y la utilidad de implementar un sistema de información que permita la utilización de los datos a efectos de la realización de estudios internacionales.

CONCLUSIONES

La nueva economía exige una rápida adaptación a los cambios. Estos se producen en todos los ámbitos, sin aviso, sin contemplaciones.

Sin perjuicio de lo expuesto al comienzo de este trabajo, esta nueva economía con las características indicadas plantea una serie de interrogantes que se irán develando con el correr del tiempo. Dichos interrogantes constituyen un llamado de atención a todos aquellos encargados del diseño de la autopista de la información.

Aún no resulta claro como los nuevos medios afectarán la manera en que la sociedad realiza sus negocios, trabaja, aprende y vive. Como se dijo anteriormente, la autopista de la información se desarrolla para proveer la infraestructura de la economía digital. Sin embargo, en la frontera digital de este nueva economía, las viejas normas sociales, leyes, regulaciones, instituciones, educación y costumbres están resultando inadecuadas.

Se plantea el interrogante de si nos convertiremos en cautivos de las nuevas tecnologías. Existe un miedo generalizado: La tecnología traerá desempleo, producirá atrofia de la mente e invasión en la privacidad.

En general se reconoce que la economía de los países pasarán de la era industrial basada en la transformación de materias primas a una nueva economía basada en el manejo de información a través de las computadoras, de la inteligencia artificial y de los recursos de la comunicación.

La era de la información transformará radicalmente las bases sobre las que descansa la economía de la sociedad argentina, al igual que lo hace en todo el mundo.

El comercio se ha visto afectado por la tecnología. A los sistemas de pago tradicionales se suman nuevos productos que transitan por un medio extraño al conocido. Dadas las características del medio, la inseguridad es la regla.

La iniciativa privada procura entonces el desarrollo de sistemas que permitan alcanzar la tan ansiada seguridad, los que son incorporados a productos como el dinero electrónico.

Como hemos visto, algunas variantes de dinero electrónico permitirían la anónima transferencia de valores. El anonimato constituiría la máxima expresión de la confidencialidad y la privacidad.

Uno de los debates más importantes en la actualidad es el relativo al "Recupero de Claves" (Key Escrow)[37]. Al analizar los principios de la criptografía

[37] El 12 de marzo de 1997 se hizo público en los Estados Unidos el proyecto "KEY RECOVERY DRAFT LEGISLATION", que contempla, en el marco de una infraestructura de administración de claves, la creación de una agencia de recupero de claves. Los interesados en obtener de una Autoridad Certificante un certificado para firmar mensajes digitalmente, deberán registrar en esta Agencia la información necesaria (clave privada) para que, en determinados casos, estos mensajes puedan ser desencriptados.

vimos como el eje central del funcionamiento de la criptografía de clave pública radica en el secreto de la clave privada. Ella solo debe ser conocida por el titular del par de claves, ya que de lo contrario el que la conociere podría firmar un mensaje (transferir valores, por ejemplo) haciéndose pasar por el titular. Se discute si los gobiernos tienen derecho a pretender acceder a las claves privadas de los usuarios, exigiendo que las mismas sean registradas, bajo el pretexto de que esta tecnología podría ser utilizada con fines ilícitos.[38]

El lavado de dinero utiliza los ámbitos más propicios para la consecución de sus fines. A medida que las operatorias tradicionales crean anticuerpos por intermedio de mayores controles, el lavado se va trasladando a otros sectores.

La transferencia electrónica de valores, a través del desarrollo de los nuevos medios de pago, podría erigirse en el campo virgen imaginado por los lavadores.

Por ello se hace necesaria la labor conjunta de los gobiernos y encargados de ejecutar las leyes y el sector privado, de forma tal que puedan implementarse y desarrollarse productos que brinden a los usuarios las garantías suficientes en cuanto a la seguridad de las operaciones, sin dejar de lado otros intereses cuyo descuido conducen al deterioro de la economía y de la sociedad.

■[38] FROOMKIN, Michael. IT CAME FROM PLANET CLIPPER: THE BATTLE OVER CRYPTOGRAPHIC KEY ESCROW, en Internet: http://www.law.miami.edu