EL SISTEMA DE SEGURIDAD JURÍDICA EN EL COMERCIO ELECTRÓNICO

Hernán Torres Álvarez

Pontificia Universidad Católica del Perú
Fondo Editorial 2005

Hernán Torres Álvarez (Lima, 1975). Abogado por la Pontificia Universidad Católica del Perú (PUCP). Se ha desempeñado profesionalmente en distintos campos del Derecho: contractual, corporativo, registral, inmobiliario y minero-ambiental. Es autor de diversos artículos sobre la seguridad jurídica en el comercio y la comunicación electrónica, que han sido publicados en diarios y revistas especializadas. Además, dicta el curso de Obligaciones en las facultades de Derecho de la PUCP y de la Universidad Femenina del Sagrado Corazón.

EL SISTEMA DE SEGURIDAD JURÍDICA EN EL COMERCIO ELECTRÓNICO

Hernán Torres Álvarez

Pontificia Universidad Católica del Perú
Fondo Editorial 2005

EL SISTEMA DE SEGURIDAD JURÍDICA EN EL COMERCIO ELECTRÓNICO

Hernán Torres Álvarez

Pontificia Universidad Católica del Perú
Fondo Editorial 2005

El sistema de seguridad jurídica en el comercio electrónico
Primera edición, febrero de 2005
Tiraje, 500 ejemplares

© Hernán Torres Álvarez, 2005

© Fondo Editorial de la Pontificia Universidad Católica del Perú, 2005
Plaza Francia 1164, Lima 1 – Perú
Teléfonos: (51 1) 330-7410; 330-7411
Fax: (51 1) 330-7405
Correo electrónico: feditor@pucp.edu.pe
Portal URL: www.pucp.edu.pe/publicaciones/fondo_ed/

Diseño de cubierta: Edgard Thays
Diagramación de interiores: Aída Nagata

Prohibida la reproducción de este libro por cualquier medio, total o parcialmente, sin permiso expreso de los editores.

ISBN 9972-42-677-7
Hecho el depósito legal 1501162004-9234 en la
Biblioteca Nacional del Perú

Impreso en el Perú – Printed in Peru

A mis padres, Hernán y Fátima; a Manuela y a Carlos, y a mis tíos,
que con su apoyo incondicional me han permitido
culminar esta, mi primera gran meta.

Contenido

Prólogo 17

Introducción 21

Capítulo I
Internet y comercio electrónico

1. Internet 27
   1.1. Introducción 27
   1.2. Reseña histórica 28
   1.3. Definición 35
   1.4. Características 36
      1.4.1. Sistema de comunicación 37
      1.4.2. Medio de tecnología subyacente 37
      1.4.3. Red abierta 37
      1.4.4. Sistema estandarizado 37
      1.4.5. Plataforma de aplicaciones 38
   1.5. Cómo conectarse a Internet 41
      1.5.1. Computadora 41
      1.5.2. *Hardware* de acceso 41
      1.5.3. *Software* de navegación 42
      1.5.4. Acceso a Internet 42
   1.6. Implicancias jurídicas del empleo de Internet 43

1.6.1. Nombres de dominio e infracciones de marcas registradas 43
1.6.2. Infracción de derechos de propiedad intelectual o industrial 44
1.6.3. Competencia desleal 44
1.6.4. Defensa de la competencia 44
1.6.5. Fraudes cometidos en la red 45
1.6.6. Conflictos de jurisdicción 45
1.6.7. Comercio electrónico 46
2. Comercio electrónico 46
2.1. Reseña histórica 46
2.2. Definición 47
2.3. Características 49
2.3.1. Medio de comercio electrónico de trascendencia económica 49
2.3.2. Medio de comercio virtual 50
2.3.3. Medio de comercio de vocación universal 50
2.3.4. Vinculación tecnológica 50
2.3.5. Medio de comercio de bajos costos 51
2.3.6. Medio de comercio rápido 51
2.4. Elementos integrantes del comercio electrónico 51
2.4.1. Los sujetos 51
2.4.2. Los actos de comercio propiamente dichos 52
2.4.3. La infraestructura de comercio electrónico 53
2.5. Niveles en el comercio electrónico 53
2.5.1. *Business to business* 54
2.5.2. *Business to consumer* 55
2.5.3. *Consumer to consumer* 57
2.5.4. *Business to government* 58
2.6. Fases en una transacción de comercio electrónico 58
2.6.1. Localización o identificación de las partes, o fase de preventa 58
2.6.2. Contratación electrónica 59
2.6.3. Ejecución y conclusión de los contratos 59

2.7. El comercio electrónico a la luz de la ley modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional 60
2.8. Dificultades en el comercio electrónico 61
2.8.1. Dificultades financieras o económicas 61
2.8.2. Dificultades jurídicas 63
2.8.3. Determinación de los problemas 64
3. Conclusiones del capítulo 68

Capítulo II
Medios de seguridad jurídica en el comercio electrónico

1. Introducción 73
2. Firma digital 74
2.1. Introducción 74
2.1.1. Funciones de la firma tradicional 74
2.1.2. Características 75
2.1.3. Elementos 75
2.1.4. Aspectos legales 76
2.1.5. Firma electrónica y firma digital 77
2.2. Definición de firma digital 78
2.3. Características de la firma digital 79
2.4. Naturaleza jurídica de la firma digital 81
2.5. Elementos de la firma digital 81
2.5.1. Datos de creación y verificación de la firma digital 81
2.5.2. Dispositivos de creación y verificación de firma digital 84
2.6. Funciones de la firma digital 88
2.7. El mecanismo de funcionamiento de la firma digital 89
2.7.1. La criptografía 89
2.7.2. Claves 92
2.7.3. Criptografía moderna 94
2.7.4. Clases 94
2.8. Función Hash 100

2.9. *Public Key Infrastructure* 105
2.10. Conclusiones 106
3. Entidades de certificación y certificados digitales 108
3.1. Introducción 108
3.2. Entidades de certificación 110
3.2.1. Definición de entidad de certificación 110
3.2.2. Características de las entidades de certificación 112
3.2.3. Funciones de las entidades de certificación 113
3.2.4. Funcionamiento de las entidades de certificación 117
3.2.5. Niveles de certificación 128
3.2.6. Naturaleza jurídica de las entidades de certificación 130
3.3. Certificado digital 132
3.3.1. Definición de certificado digital 132
3.3.2. Características del certificado digital 133
3.3.3. Funciones del certificado digital 135
3.3.4. Contenido del certificado digital 136
3.3.5. Clases de certificados digitales 138
3.3.6. Vigencia de los certificados digitales 139
3.3.7. Equivalencia de certificados digitales 143
3.3.8. Naturaleza jurídica del certificado digital 145
3.4. Conclusiones 145
4. Los medios de pago electrónicos 147
4.1. Introducción 147
4.2. Aspectos jurídicos del pago 149
4.2.1. Definición de pago 149
4.2.2. Requisitos de pago 150
4.2.3. Efectos del pago 151
4.2.4. Naturaleza jurídica del pago 152
4.3. Medios de pago electrónicos 152
4.3.1. Definición de medios de pago electrónicos 152
4.3.2. Características de los medios de pago electrónicos 153
4.3.3. Seguridad digital 155
4.3.4. Naturaleza jurídica de los medios de pago electrónicos 160

4.3.5. Clasificación de los medios de pago electrónicos 161
4.4. Principales medios de pago 162
4.4.1. Tarjeta electrónica 162
4.5. Dinero electrónico 184
4.5.1. Definición de dinero electrónico 184
4.5.2. Sujetos participantes en el empleo del dinero electrónico 186
4.5.3. Creación del dinero electrónico 186
4.5.4. Requisitos para el empleo del dinero electrónico 188
4.5.5. Pago mediante dinero electrónico 188
4.5.6. Ventajas y desventajas en el empleo del dinero electrónico 190
4.6. Pagos mediante teléfono móvil 194
4.6.1. Introducción 194
4.6.2. Ventajas del pago mediante teléfono móvil 194
4.6.3. Funcionamiento del pago mediante teléfono móvil 195
4.6.4. Tipos de pago móvil 195
4.6.5. Modalidades del pago móvil 195
4.7. Principales medios de pago electrónico en el mercado mundial 198
4.7.1. Sistemas *card-based* 198
4.7.2. Sistemas *software-based* 198
4.7.3. Sistemas por puntos 199
4.7.4. Sistemas *e-mail money* 199
4.8. Conclusiones 204
4.9. La biometría 208
4.9.1. Introducción 208
4.9.2. Definición de biometría 209
4.9.3. Características de la biometría 209
4.9.4. Ventajas y desventajas del empleo de la biometría 210
4.9.5. Técnicas de autenticación biométrica 211
4.9.6. Naturaleza jurídica de la biometría 213

4.9.7. Viabilidad de la biometría para formar parte del sistema de seguridad jurídica en el comercio electrónico 213
4.10. Conclusiones 214
5. Conclusiones del capítulo 215

Capítulo III
Sistema de seguridad jurídica en el comercio electrónico

1. Introducción 219
2. Definición 222
2.1. Medios de seguridad electrónicos 223
2.2. Principios de seguridad jurídica en el comercio electrónico 223
2.3. Seguridad jurídica 224
3. Características 225
4. Funciones del sistema de seguridad jurídica en el comercio electrónico 227
4.1. Función de identificación de los sujetos del comercio electrónico 227
4.2. Función de identificación de los mensajes transmitidos 227
4.3. Función de vinculación de los sujetos 228
4.4. Función de oponibilidad del pago electrónico 229
4.5. Función probatoria 229
4.6. Función de intermediación 230
4.6.1. Función facultativa 231
4.6.2. Tercero neutral 232
4.6.3. Objetivos 233
4.6.4. Función pública 233
5. Funcionamiento del sistema de seguridad jurídica en el comercio electrónico 234
5.1. Requisitos para el funcionamiento del sistema de seguridad jurídica en el comercio electrónico 234
5.2. Funcionamiento del sistema de seguridad jurídica en el comercio electrónico 235

5.2.1. Envío de mensaje firmado digitalmente 235
5.2.2. Envío de mensaje cifrado 236
5.2.3. Envío de mensaje autenticado 237
5.2.4. Funcionamiento del sistema de seguridad jurídica en el comercio electrónico 241
5.3. Modelo de transacción de comercio electrónico con el sistema del mensaje autenticado 244
5.3.1. Etapa de contratación electrónica entre el comerciante y el consumidor. Fases 1 a 8 244
5.3.2. Etapa de contratación entre el consumidor y su banco. Fases 9 a 12 245
5.3.3. Etapa de emisión de dinero electrónico. Fases 13 a 15 247
5.3.4. Etapa de pago con dinero electrónico. Fases 16 a 21 247
6. Principios que regulan el funcionamiento del sistema de seguridad jurídica en el comercio electrónico 248
6.1. Principio de neutralidad tecnológica 248
6.2. Principio de equivalencia funcional 249
6.3. Principio del valor probatorio del documento electrónico 251
6.3.1. Principio de prueba libre previa autorización judicial 251
6.3.2. Principio de prueba tasada 251
6.3.3. Principio de libre convicción 251
6.3.4. Autonomía de la voluntad 252
6.4. Principio de actuación subsidiaria del Estado 252
7. Conclusiones del capítulo 253

Capítulo IV
Conclusiones 257

Bibliografía 275

Prólogo

Hernán Torres Álvarez me ha honrado al pedirme que prologue su primer libro, *El sistema de seguridad jurídica en el comercio electrónico*, solicitud que acepté de inmediato por dos razones: la gran amistad que me une a quien fue uno de mis alumnos más destacados en la Facultad de Derecho de la Pontificia Universidad Católica del Perú (PUCP), y la calidad y originalidad de su obra.

Antes de empezar a escribir este libro, Hernán compartió conmigo sus inquietudes sobre la contratación electrónica porque siempre tuve un vivo interés en la materia, que empezó en 1995, cuando escribí *Las doctrinas tradicionales frente a la contratación computarizada (Análisis del funcionamiento de las doctrinas tradicionales sobre consentimiento, nulidad, anulabilidad y disentimiento en los contratos celebrados a través de medios informáticos)*, y se reforzó posteriormente con la publicación de *Tratado de la Teoría General de los Contratos. La plena vigencia del Código Civil en la contratación contemporánea* en 2002.

En esas obras, me centré en el aspecto sustantivo de la contratación computarizada y confronté las doctrinas contractuales vigentes con los avances de la tecnología en lo que respecta a los medios electrónicos que facilitan esta actividad en nuestros días. Si bien concluí que en el mundo moderno se siguen aplicando casi todas las doctrinas tradicionales, siempre tuve conciencia de que hay un aspecto que se mantiene inexplorado. Me refiero a la seguridad jurídica en la contratación computarizada, que constituye un gran

vacío tanto en la cátedra como en la investigación, y que siempre me pareció necesario que fuera cubierto lo más pronto posible y de la mejor manera. Así, cuando Hernán me comentó que planeaba escribir sobre este tema, solo me cupo alentarlo.

Debo confesar también que mi asesoría en la materia fue mínima, puesto que cada vez que Hernán me alcanzaba sus borradores, yo constataba que estaban muy bien escritos y que en ellos se reflejaba un gran esfuerzo y el aporte de muchas obras de consulta. Así pues, más que un asesor, me convertí en un lector atento a aquello que aprendía conforme avanzaba en la revisión del texto.

En esta obra, el autor analiza rigurosamente las materias que aborda, combinando de manera notable los aspectos técnicos y jurídicos de las nuevas tecnologías de la información y la comunicación. Y es que el Derecho no puede prescindir de las nuevas tecnologías, así como tampoco estas pueden prescindir del Derecho, en la medida en que esa evolución científica cotidiana necesita indefectiblemente un soporte jurídico en la sociedad.

Y así como en la historia del Derecho el papel cumplió una función muy importante —para dejar constancia de la celebración de actos jurídicos y también para servir de medio probatorio del pago realizado—, no cabe duda de que, con el paso de los años —sobre todo en las últimas dos décadas—, este material ha ido compartiendo el protagonismo con los medios electrónicos tanto para la celebración de actos jurídicos como para acreditar la ejecución de estos. No es que el papel haya desaparecido o vaya a desaparecer de manera inminente, sino que no podemos dejar de reconocer que, paulatinamente, su importancia decrece; con frecuencia, las nuevas generaciones prefieren leer los textos en CD-ROM y han hecho de Internet y sus fascinantes posibilidades parte inseparable de su forma de vivir.

Tal vez quienes no crecimos bajo el influjo de las computadoras seamos los que más nos aferramos al uso del papel. Sin embargo, no podemos evitar que la humanidad se dirija hacia la utilización de los medios electrónicos para todo, inclusive para realizar aquellas operaciones que siempre consideramos imposibles de desligar

de aquel soporte. Hace algunos años resultaba inimaginable un mundo en el que los contratos importantes no fueran registrados en papel o, en el caso de los principales, no se elevaran a escritura pública; hoy, en cambio, las nuevas tecnologías de la comunicación y la información están haciendo que esta situación varíe notablemente.

Advirtiendo esta realidad y luego de dedicar el primer capítulo a hacer un estudio preliminar sobre Internet y el comercio electrónico, el autor aborda en el segundo capítulo los medios de seguridad jurídica en el comercio electrónico, para lo cual parte del tema de la firma digital. Describe sus funciones, características, elementos y aspectos legales, y la distingue de la firma electrónica. Además, analiza otros temas de sumo interés, como el relativo al mecanismo de funcionamiento de la firma digital.

En este mismo capítulo, estudia las entidades de certificación y los certificados digitales. Analiza los aspectos generales y las características de los principales medios de pago electrónicos utilizados en el mercado mundial y algunos usos derivados de la biometría.

En el tercer capítulo aborda el sistema de seguridad jurídica en el comercio electrónico, señalando cuáles son los medios de seguridad electrónicos, los principios de seguridad jurídica, las características del sistema y sus diversas funciones —identificación de los sujetos del comercio y de los mensajes, vinculación de los sujetos, oponibilidad del pago electrónico, función probatoria e instrumento de intermediación—, y posteriormente estudia el funcionamiento de este sistema tanto en lo referente a sus requisitos como a su funcionamiento propiamente dicho.

Finalmente, se refiere a los principios que regulan el funcionamiento del sistema de seguridad jurídica en el comercio electrónico: el de neutralidad tecnológica, el de equivalencia funcional, el del valor probatorio del documento electrónico y el de actuación subsidiaria del Estado.

En vista del muy apreciable número de transacciones que se realizan en nuestros tiempos a través de medios electrónicos y considerando que una de las funciones primordiales del Derecho consiste en brindar seguridad jurídica a la sociedad, la obra de

Hernán Torres Álvarez resulta verdaderamente importante y pionera en el Perú.

Durante las décadas de 1980 y 1990, el Derecho estuvo ocupado en adecuarse a los medios de contratación electrónica y en verificar cómo podía funcionar en ellos. Una vez salvados estos obstáculos teóricos, es necesario adecuar los nuevos actos electrónicos a las formalidades jurídicamente relevantes en materia probatoria, que brinden a los usuarios las garantías necesarias para celebrar sus transacciones a través de estos medios. Al brindar seguridad jurídica, el Derecho busca que, sea cual sea la vía que las partes utilicen para contratar, siempre tengan garantías suficientes para actuar sin temor.

En esta línea se inscribe la obra de Hernán Torres, quien como dije al principio, fue mi alumno en la PUCP hace pocos años y hoy, además de ejercer la profesión en uno de los más antiguos y respetados estudios de abogados de la capital, ha ingresado a la docencia en su propia alma máter, al confiársele el dictado de uno de los horarios del curso Derecho de las Obligaciones, una de las materias más complejas y fascinantes del Derecho.

Reitero mi agradecimiento a Hernán por haberme pedido prologar esta obra y lo felicito por la calidad de su trabajo y por el interesante y novedoso tema que aborda.

Mario Castillo Freyre

Introducción

La tecnología es, sin duda, uno de los factores que más han contribuido a los cambios sociales, políticos y económicos en la historia de la humanidad. Son innumerables las invenciones tecnológicas que han aportado a este cambio. Sin embargo, no todas las invenciones han tenido la misma participación y trascendencia en el cambio y evolución del hombre. La rueda, la imprenta, la luz eléctrica, el teléfono y la radio, entre otras, son invenciones tecnológicas que, como la historia puede corroborar, han modificado trascendentalmente la vida y las costumbres del ser humano.

Los cambios producidos por estas invenciones tecnológicas en la vida de los hombres han traído consigo aspectos positivos, que sin duda alguna han conllevado la necesidad de ser regulados por normas que permitan su plasmación eficiente en el contexto social de su aplicación. En este sentido, la participación del Derecho en los cambios sociales que genera la aparición de novedades tecnológicas siempre ha sido necesaria. En efecto, el Derecho debe regular los efectos e implicancias de estas novedades a fin de adaptarlas a las estructuras sociales. Además, debe evitar en lo posible la aparición de conflictos o, si es que aparecen, determinar posibles mecanismos de solución.

El Derecho, como herramienta reguladora de paz y orden social, es de vital importancia para lograr que los cambios que traen consigo las nuevas tecnologías no generen efectos adversos. Del

mismo modo, el Derecho es una herramienta para incentivar el empleo de nuevas tecnologías al garantizar a sus usuarios que se producirán los fines deseados, evitando los efectos perjudiciales. Al mismo tiempo, puede ser una herramienta que desaliente el empleo de tecnologías que se consideren nocivas para los intereses de la sociedad.[1]

Sin duda, Internet se ha convertido en los últimos años en la invención tecnológica que más cambios ha traído consigo, tanto en los hábitos como en las costumbres sociales de toda esfera. Tanto en el comercio como en la educación, el entretenimiento, la salud y la información, Internet es el medio tecnológico que ha revolucionado la vida del hombre en los últimos cinco o diez años, y promete continuar contribuyendo en forma determinante con el cambio y la evolución social.

Al tener Internet un papel protagónico en nuestra sociedad, es vital la participación del Derecho mediante la regulación de los cambios sociales que se produzcan. Sin embargo, ya desde el inicio, el mundo jurídico se encuentra con un obstáculo de considerable importancia y difícil superación. Este obstáculo es la rapidez con la que evoluciona la tecnología y con la que se producen los cambios sociales que Internet trae consigo. Lamentablemente, el Derecho, como instrumento que refleja la realidad y la proyección social de una sociedad determinada, no avanza ni evoluciona con la misma rapidez con que lo hacen las invenciones tecnológicas.

Por ello, es necesario dotar al Derecho de mecanismos que le permitan una rápida adaptación a los cambios tecnológicos y a los consiguientes cambios sociales que se produzcan, a fin de permitir su efectiva regulación y canalización.

Como hemos señalado, Internet influye en casi todos los ámbitos y esferas de la sociedad. Sin embargo, la esfera económica está entre las que han experimentado mayor evolución. La aplicación

---

[1] Por ejemplo, en la actualidad es materia de discusión si es que el Derecho debe prohibir la clonación de personas.

económica de Internet es, definitivamente, una de las que más cambios han sufrido, y a una velocidad impresionante. Nos referimos al comercio electrónico o *e-commerce*. La realización del comercio electrónico ha traído cambios estructurales en las transacciones comerciales locales e internacionales. Tanto es así que se distingue entre comercio tradicional y comercio electrónico; el primero es el que no se realiza con medios electrónicos.

El comercio electrónico se caracteriza por su celeridad, su flexibilidad y su universalidad en la realización de transacciones comerciales. Es al mismo tiempo un medio de comercio económico, gracias a sus bajos costos, e ideal para la celeridad que requieren las operaciones comerciales. Sin embargo, así como presenta grandes ventajas, trae consigo una serie de obstáculos tecnológicos y legales que dificultan su óptimo funcionamiento.

Al ponderar la importancia de Internet y del comercio electrónico, nos hemos visto motivados a realizar un estudio de estos temas para determinar, desde una perspectiva jurídica, cuáles son sus principales características, así como los problemas jurídicos que se plantean con su implementación y uso. La finalidad es ofrecer a estudiantes y operadores del Derecho un acercamiento a estos temas, que consideramos de trascendental importancia.

Uno de los principales objetivos del Derecho en la regulación del comercio electrónico es dotarlo de seguridad. Este objetivo se puede lograr con la aplicación de un sistema de seguridad jurídica —que proponemos en este trabajo y que será descrito más adelante— que está diseñado para trascender en el tiempo y no sufrir el desfase del Derecho que el avance tecnológico produce. Al ser Internet una herramienta de comercio tan importante, será necesario que los operadores del Derecho conozcan de cerca sus principales implicancias, para que puedan emplear y crear mecanismos que permitan superar los obstáculos que se presenten.

A lo largo de la investigación hemos encontrado que cada problema u obstáculo que se presenta tiene su correlato en un medio tecnológico determinado, cuyo funcionamiento y concepción son individuales. Este hecho ofrece una seguridad incompleta en

términos jurídicos. La seguridad jurídica implica la concepción de seguridad en conjunto, no limitada exclusivamente a un aspecto. Por este motivo, en este trabajo hemos tratado de explicar jurídicamente, en primer lugar, el funcionamiento individual de los medios de seguridad. Luego hemos planteado la posibilidad teórica del funcionamiento conjunto de estos medios individuales en un sistema integral de seguridad, que hemos denominado Sistema de Seguridad Jurídica en el Comercio Electrónico (SSJ) y que tiene sus propios principios de funcionamiento.

Debemos señalar que este sistema integral es un planteamiento teórico. Se trata de un intento de explicar el funcionamiento de medios tecnológicos de seguridad y de darles una forma jurídica. Por esta razón, pueden existir otros tipos de sistemas o de concepciones de seguridad jurídica en el *e-commerce*.

Este trabajo tiene dos objetivos fundamentales. En primer lugar, introducir a los estudiantes y operadores del Derecho a Internet y al comercio electrónico desde una perspectiva jurídica. En segundo lugar, realizar un estudio sobre la seguridad jurídica del comercio electrónico. Para lograrlo, en primer término hemos detectado los principales problemas legales que se presentan en este tipo de comercio y cuáles son los medios tecnológicos que permiten superarlos. En segundo término hemos dado una explicación del funcionamiento individual de estos medios tecnológicos desde una perspectiva jurídica, para luego plantear la posibilidad teórica de una concepción y de un funcionamiento integral de los medios tecnológicos que permitan alcanzar la tan anhelada seguridad jurídica en las operaciones comerciales mediante Internet.

Para lograr los objetivos señalados hemos dividido este trabajo en cuatro capítulos. El primero es un capítulo introductorio, en el que se aborda los temas de Internet (que es el soporte tecnológico del *e-commerce*) y de comercio electrónico. Se señala como principal problema la falta de seguridad jurídica en las operaciones de *e-commerce*. En el segundo capítulo estudiamos los medios de seguridad que la tecnología ha desarrollado para superar el problema de la seguridad jurídica. Se trata de un problema que abarca diversos

aspectos y para cuya solución existe un medio tecnológico específico, aunque está limitado en su aplicación individual. En el tercer capítulo se desarrolla nuestra propuesta de lo que llamamos Sistema de Seguridad Jurídica (SSJ), que básicamente funciona con la aplicación en conjunto de los medios de seguridad estudiados en el capítulo segundo, cuya capacidad de proporcionar seguridad, como hemos indicado, está limitada cuando son aplicados individualmente. El cuarto y último capítulo contiene las conclusiones de este trabajo.

Por último, consideramos necesario resaltar que este texto tiene como objetivo adicional incentivar la difusión del conocimiento en materia de comercio electrónico desde una perspectiva jurídica, además de estudios posteriores sobre los temas de esta materia que aquí no hayan sido abordados en profundidad.

CAPÍTULO I
INTERNET Y COMERCIO ELECTRÓNICO

1. INTERNET

1.1. Introducción

> La llegada de Internet se ha descrito ampliamente como algo tan importante para la sociedad como el desarrollo del computador personal, el teléfono o incluso la prensa escrita. Aun así, es difícil explicar a los que no han utilizado nunca Internet su capacidad para cambiar la vida, crear nuevas empresas o acercar familias muy separadas. Para los que han empezado a utilizar Internet y han superado las frustraciones iniciales asociadas a la utilización de toda nueva tecnología, Internet puede hacer todo eso y mucho más.
>
> Unión Internacional de Telecomunicaciones. «Cuál es la Singularidad en Internet». En <http://www.itu.int/newsroom/wtd/2001/ExecutiveSummary-es.html>.

Iniciamos la introducción en el tema de Internet citando un documento de trabajo elaborado con motivo de la Celebración del Día Mundial de las Telecomunicaciones.[1] Si bien esta cita puede dar a entender que Internet es la panacea para los problemas sociales, económicos y culturales —opinión que no compartimos—, nos es útil para graficar la importancia y la trascendencia de Internet en

[1] 17 de mayo de 2001.

nuestra sociedad, además de la manera en que este aporte tecnológico ha influido en ella.

Como hemos señalado en la introducción de este trabajo, es necesario entender el funcionamiento del soporte tecnológico mediante el cual se llevan cabo las relaciones de comercio electrónico. Es indudable que es Internet lo que ha permitido la rápida expansión y desarrollo del *e-commerce*. Por este motivo, es indispensable conocer sus características y su funcionamiento, y, sobre todo, comprender las implicancias jurídicas que representa este medio tecnológico.

Para lograr este cometido, en este capítulo describiremos las características y el funcionamiento de Internet.

1.2. Reseña histórica

Inicialmente, Internet fue concebido como un mecanismo de comunicaciones para el ámbito militar. Su objetivo era permitir contar con redes de comunicación fácilmente trasladables y que no requiriesen de una complicada infraestructura.

Nos es muy útil la descripción de la evolución de Internet realizada por Barrios Osorio:

> Las redes de computadoras funcionaban con el principio de una computadora central o servidor, y terminales conectadas a la central. Si fallaba el servidor, fallaba la red completa. Esto limitaba la interconexión a distancia, y es así como en los inicios de la década del sesenta el Departamento de Defensa de los Estados Unidos de América crea, a través de la Agencia de Desarrollo de Proyectos Avanzados —RPA— (*Advanced Research Project Agency*), un proyecto que buscaba interconectar computadoras formando una red, pero que tuvieran la capacidad de funcionar aunque otras estuvieran fuera de servicio. Surge el proyecto ARPANET, que en sus inicios funcionó con un programa de computación denominado *Network Control Protocol* —NPC—, lo que hizo que la red experimental funcionara descentralizadamente; una de sus ventajas principales era que se podía conectar con diferentes tipos de computadoras (*hardware*) y de programas (*software*). En la década de 1980, DARPA patrocinó el desarrollo de un nuevo protocolo que sustituye al NPC, denominado *Transmission Control Protocol / Internetworking*

> *Protocol*, identificado por sus siglas TCP/IP, funcionando como una red independiente.
>
> A principios de la década de los ochenta, el naciente Internet se separa de ARPANET, desligándose de los objetivos militares para los que fue concebida inicialmente, tomando un aire eminentemente académico, y se funda la *National Science Foundation Network* —NSFNET—, financiada por el Gobierno Federal de Estados Unidos de América, iniciando en ese momento la oportunidad para que cada centro universitario estableciera una conexión.
>
> Se establecieron enlaces denominados *Backbones* (columna vertebral) y empezó su expansión fuera de Estados Unidos. La NSFNET intento imponer una Política de Uso Aceptable (*Acceptable Use Policy*), con el objetivo de que Internet se utilizara solo para propósitos científicos y académicos, no de usos comerciales, pero no se logró este objetivo; hay que recordar que gracias al comercio Internet tiene desde 1995 un crecimiento constante y enorme.[2]

Para complementar esta reseña es preciso señalar que hasta el advenimiento de la *World Wide Web* (red de cobertura mundial), en 1990, Internet fue casi completamente desconocido fuera de las universidades y de los departamentos de investigaciones de las corporaciones. Se accedía a ella principalmente sirviéndose de un programa que permitía la comunicación solo entre dos computadoras y no de manera simultánea sino sucesiva. Desde entonces Internet ha crecido hasta convertirse en un sistema de información y de comercio casi imprescindible. En la actualidad, es ampliamente aceptada para la realización de actividades comerciales como publicidad, ventas en línea o servicios en línea. Señala Ramos Suárez:

> En los últimos años, Internet ha experimentado un crecimiento exponencial en el número de usuarios y hoy en día está consolidándose como un medio de comunicación habitual en la mayoría de países. El auge de Internet está propiciando la aparición de una serie de servicios cuya característica principal es la oferta de los mismos a distancia, es

---

[2] BARRIOS OSORIO, Omar. «Internet y Derecho. Fundamentos de una relación». En <http://vlex.com/redi/No._35_-_Junio_del_2001/12>.

decir, a través de la red. Esta actividad no es otra que el tan denominado y citado «comercio electrónico o electronic commerce».[3]

A pesar de que Internet ha cobrado vital importancia, su espíritu original de cooperación y de libertad ha sobrevivido a esta explosiva transformación. Lo demuestra el hecho de que la vasta mayoría de información disponible en Internet sea libre de costo. La web es el aspecto más conocido de Internet. Sin embargo, existen otras aplicaciones, como el correo electrónico, el *chat* y la transferencia de archivos.

Para demostrar el aporte de Internet en los ámbitos mencionados, señalaremos algunos datos estadísticos:

Ventas al público

Ventajas	Internet (%)	Catálogos (%)	Tiendas (%)
Precios más competitivos	21	10	13
Todo se puede comprar en un solo lugar	12	7	13
Conveniencia	59	41	12
Ahorro de tiempo	62	33	3

Fuente: Andersen Consulting

Reducción de costos

Evaluación de costos en Internet

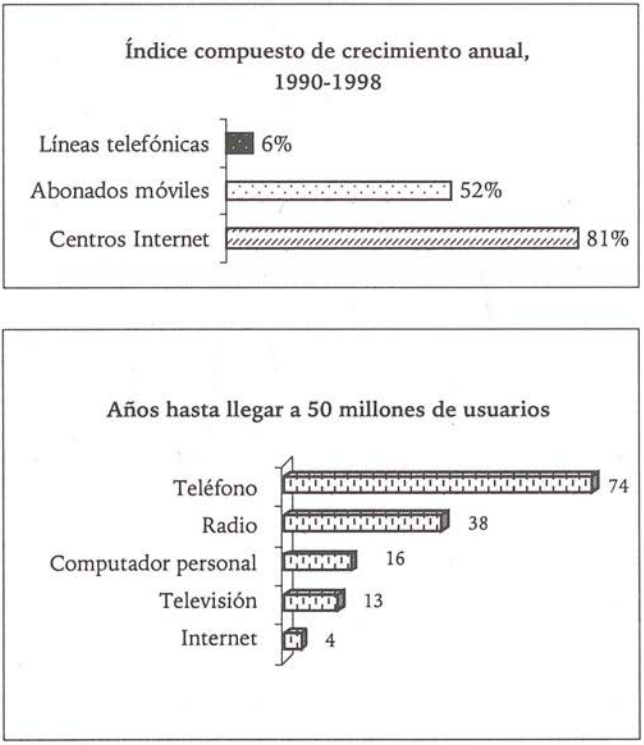
Concepto	Detalle	US$	Tiempo
Transacción de corretaje	*Full service*	150,00	
	Discount broker	69,00	
	Online broker	10,00	
Transacción bancaria tradicional	*Branch*	1,27	
	ATM	0,27	
	Internet	0,01	
Envío de documento de 42 páginas de Ottawa a Tokio	*Courier*	39,00	24 horas
	Fax	24,49	31 minutos
	Internet	0,11	2 minutos

Fuente: Andersen Consulting

[3] RAMOS SUÁREZ, Fernando. «El comercio electrónico: la seguridad técnica y jurídica». En <http://www.masterdisseny.com/master-net/legalia/0006.php3>.

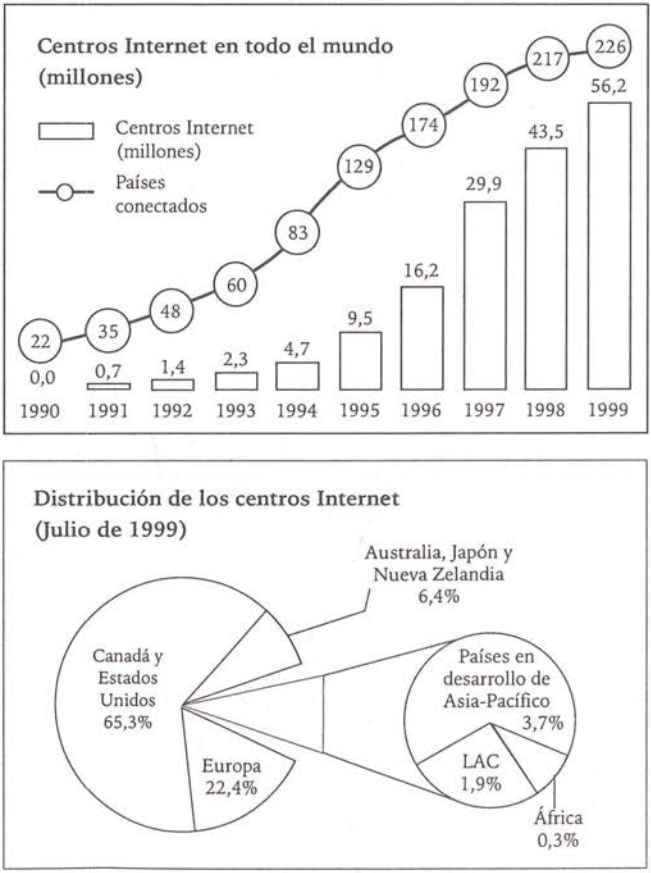
Por las ventajas señaladas, la expansión en el empleo de Internet ha sido muy importante en los últimos años, como se puede apreciar en las figuras 1 y 2, y en el siguiente cuadro.

Figura 1. Crecimiento de Internet: ya no es exponencial, pero continúa siendo impresionante
Índices de crecimiento acumulativo anual (de 1990 a 1998) y número de años hasta alcanzar 50 millones de usuarios.



Fuente: Banco de Datos de la UIT de indicadores mundiales de las telecomunicaciones, Network Wizards, Compaq, RIPE.

Figura 2. La red crece pero de forma desigual
Base instalada de centros Internet (de enero de 1991 a julio de 1999) y distribución por regiones para julio de 1999.



Nota: los datos del gráfico de la parte superior se refieren a enero del año siguiente. Se utilizó un nuevo método para calcular el número de computadoras centrales Internet a partir de enero de 1998. Las inscripciones de dominios de nivel superior genérico (gTLD) se distribuyen entre países según las inscripciones de septiembre de 1997.

*Datos de julio de 1999. LAC: América Latina y el Caribe.

Fuente: UIT. Los datos sobre las computadoras centrales Internet se han adaptado de Network Wizards (<http://www.nw.com>) y de RIPE (<http://www.ripe.net>). Los datos correspondientes a los países conectados proceden de Internet Society.

País o región	Población (2003)	Usuarios, dato más reciente	Crecimiento (2000-2003)	Porcentaje población (penetración)	Fecha del dato más reciente	Tabla (%)
Estados Unidos	291.639.900	179.854.855	88,6%	61,7	julio 2003	26,6
China	1.311.863.500	68.000.000	202,2%	5,2	junio 2003	10,1
Japón	127.708.000	59.203.896	25,8%	46,4	junio 2003	8,8
Alemania	81.904.100	44.139.062	83,9%	53,9	junio 2003	6,5
Reino Unido	59.040.300	34.387.216	123,3%	58,2	junio 2003	5,1
Corea del Sur	46.852.300	26.270.000	38,0%	56,1	diciemb. 2002	3,9
Francia	59.303.800	21.309.352	150,7%	35,9	julio 2003	3,2
Italia	56.209.900	19.250.000	45,8%	34,2	agosto 2001	2,8
Canadá	31.720.400	16.841.811	32,6%	53,1	marzo 2003	2,5
India	1.067.421.100	16.580.000	231,6%	1,6	diciemb. 2002	2,5
Brasil	179.712.500	14.322.367	186,4%	8,0	julio 2003	2,1
España	41.547.400	13.986.724	159,6%	33,7	julio 2003	2,1
Australia	19.978.100	12.823.848	94,3%	64,2	junio 2003	1,9
Taiwán	23.614.200	11.602.523	85,3%	49,1	julio 2001	1,7
Holanda	16.258.300	10.351.064	165,4%	63,7	junio 2003	1,5
Malasia	24.014.200	7.800.000	110,8%	32,5	junio 2003	1,2
Suecia	8.872.600	6.726.814	48,9%	67,9	mayo 2003	0,9
Rusia	141.364.200	6.000.000	93,5%	4,2	diciemb. 2002	26,6
Turquía	73.197.200	4.900.000	145,0%	6,7	diciemb. 2002	0,7
Tailandia	63.393.600	4.800.000	108,7%	7,6	diciemb. 2002	0,7
México	101.457.200	4.663.400	71,9%	4,6	diciemb. 2002	0,7
Hong Kong	6.827.000	4.571.536	100,2%	67,0	junio 2003	0,7

País o región	Población (2003)	Usuarios, dato más reciente	Crecimiento (2000-2003)	Porcentaje población (penetración)	Fecha del dato más reciente	Tabla (%)
Suiza	7.376.000	4.271.998	100,2%	57,9	junio 2003	0,6
Argentina	36.993.000	4.100.000	64,0%	11,1	diciemb. 2002	0,6
Indonesia	217.825.400	4.000.000	100,0%	1,8	diciemb. 2001	0,6
Los 25 países líderes	4.096.094.200	600.756.466	89,7%	14,7	septiemb. 2003	88,7
Los 208 países restantes	2.252.168.310	76.270.608	72,4%	3,4	septiemb. 2003	11,3
Total mundial de usuarios	6.348.262.510	677.027.074	87,6%	10,7	septiemb. 2003	100,0

Notas:

- Estos datos fueron actualizados el 19 de septiembre de 2003.
- Las cifras en detalle se pueden consultar en las páginas correspondientes a cada región y país.
- Las cifras de población se basan en los datos actuales de <http://www.gazetteer.de/home.htm>.
- Los datos más recientes de usuarios corresponden a datos de <http://www.nielsen-netratings.com>, de ITU y de otras fuentes locales.
- Las cifras comparativas de crecimiento se determinaron con el dato actual de usuarios frente al dato del año 2000, tomado de las estadísticas del ITU.
- Se autoriza la reproducción de los datos, siempre y cuando se cite la fuente original y se establezca un enlace a <http://www.exitoexportador.com>.

América del Sur	Población actual (2003)	Usuarios (año 2000)	Usuarios (dato más reciente)	Tabla (%)	Crecimiento (2000 a 2003)	Porcentaje población (penetración)
Argentina	36.993.000	2.500.000	4.100.000	14,6	64,0%	11,1
Bolivia	8.676.000	120.000	180.000	0,6	50,0%	2,1
Brasil	179.712.500	5.000.000	14.322.367	51,0	186,4%	8,0
Chile	15.265.600	1.757.400	3.102.200	11,0	76,5%	20,3
Colombia	44.533.300	878.000	1.982.000	7,1	125,7%	4,5
Ecuador	12.471.600	180.000	503.300	1,8	179,6%	4,0
Guayana Francesa	188.200	2.000	2.000	0,0	0,0%	1,1
Guyana	865.200	3.000	95.000	0,3	3.066,7%	11,0
Islas Malvinas	2.300	–	–	0,0	–	n/d
Paraguay	6.028.900	20.000	100.000	0,4	400,0%	1,7
Perú	27.083.400	2.500.000	2.000.000	7,1	-20,0%	7,4
Surinam	456.900	11.700	14.500	0,1	23,9%	3,2
Uruguay	3.452.600	370.000	400.000	1,4	8,1%	11,6
Venezuela	23.865.800	950.000	1.274.400	4,5	34,1%	5,3
Total Sudamérica	**359.595.300**	**14.292.100**	**28.075.767**	**100,0**	**96,4%**	**7,8**

Fuente: Éxito Exportador (<http://www.exitoexportador.com/index.html>). Se trata de un directorio que contiene información, herramientas y recursos para las exportaciones vía Internet. Ofrece datos actualizados del número proyectado de usuarios del Internet en 238 países y regiones, además de la población mundial actual, el ingreso per cápita, mapas, buscadores y distintos enlaces.

1.3. Definición

Resulta complicado definir Internet debido a sus múltiples factores y funciones, y a los distintos conceptos que se tienen de él. Incluso podríamos afirmar que existen tantas definiciones de Internet como usuarios existan en la red. Sin embargo, tomaremos algunas definiciones para luego complementarlas y elaborar una síntesis.

En cuanto al origen de la palabra «Internet», tenemos que es un apócope de *Interwork System* (Sistema e Intercomunicación de Redes).

Para algunos técnicos, sin embargo, el término «Internet» es una contracción de *INTERnational NET*.[4]

Según el doctor Víctor Rojas Amando, citado por Barrios Osorio, «Internet es un sistema maestro de diversas redes de computación que cumple dos funciones básicas: medio de comunicación y medio de información».[5]

La siguiente definición tiene una naturaleza descriptiva:

> La red de computadoras más extendida del planeta, que conecta y comunica a más de 50 millones de personas. Su estructura técnica se basa en millones de computadoras que ofrecen todo tipo de información. Estas computadoras, encendidas las 24 horas, se llaman servidores y están interconectadas entre sí en todo el mundo a través de diferentes mecanismos de líneas dedicadas, sin importar qué tipo de computadoras son, para intercomunicarse utilizan el protocolo TCP/IP. Las computadoras que utilizan las personas para conectarse y consultar los datos de los servidores se llaman clientes, y acceden en general a través en un tipo de conexión llamado *dial-in*, utilizando un módem y una línea telefónica.[6]

Teniendo en cuenta estas dos definiciones, podemos concluir que Internet es un sistema de comunicación compuesto por un conjunto de computadoras-servidores. Estas se encuentran interconectadas e interactúan dentro de un medio llamado *red*, mediante el empleo de un protocolo común, al cual tienen acceso otras computadoras llamadas *usuarios*. Ofrece una serie de aplicaciones que permiten a los usuarios comunicarse y tener acceso a todo tipo de información.

1.4. Características

Según esta definición, Internet tiene las siguientes características:

---

[4] BARRIOS OSORIO. Ob. cit.

[5] Ibíd.

[6] BASSI, Roxana. «Diccionario de Internet». En: *Internet World*. <http:/www.iworld. com.ar/>.

1.4.1. Sistema de comunicación

Es un sistema que tiene por objeto la comunicación y el acceso a la información. Está formado por un conjunto de computadoras que se relacionan entre sí de acuerdo con protocolos establecidos. En otras palabras, existe una lógica y un orden en el funcionamiento de Internet. Esta lógica, como se ha señalado, está incorporada en el protocolo TCP/IP.

Este sistema está integrado por cuatro elementos: las computadoras-servidores, las computadoras-usuarios, los protocolos y los prestadores de servicios de Internet (PSI).

1.4.2. Medio de tecnología subyacente

La existencia y el funcionamiento de Internet están en íntima relación con otros medios tecnológicos. Se trata del *software* y el *hardware* necesarios para la efectiva conexión a la red.[7]

1.4.3. Red abierta

Internet es un medio de comunicación, una red a la cual tienen acceso las personas que tengan los medios tecnológicos adecuados (*software* y *hardware*). Se trata de un medio de comunicación de libre acceso, abierto y público; no es un medio cerrado.

1.4.4. Sistema estandarizado

Puesto que se trata de una red abierta de comunicaciones e información, Internet requiere de protocolos, tecnologías y lenguajes comunes para un funcionamiento eficiente. En cuanto a los protocolos, como se ha señalado, el más usado es el TCP/IP. La tecnología, es decir, el *software* y el *hardware*, es múltiple y cambiante. En

---

[7] *Software* es el programa o conjunto de programas que se utilizan en computación para procesar datos e información (sistemas operativos como DOS, paquetes como Office y programas como Word y Excel). *Hardware* es el conjunto de elementos físicos que integran una computadora (el monitor, el disco duro, el teclado, el módem, etc.).

cuanto al idioma, el inglés es el que se ha impuesto, debido al origen de Internet. Este hecho podría ser un obstáculo para el desarrollo de Internet. Sin embargo, este inconveniente es parcialmente resuelto por servicios de traducción como el que provee <http:/ www.bebelfish.altavista.digital.com/>.

1.4.5. Plataforma de aplicaciones

Como hemos indicado, Internet permite la comunicación y el acceso a la información mediante diversas funciones, llamadas *aplicaciones*. Las principales son las siguientes:

- *World Wide Web* (WWW)

Es la aplicación más utilizada de Internet. Es un sistema de información en línea, basado en los enlaces de hipertexto (las páginas web están entrelazadas por medio de palabras o imágenes que permiten acceder a otros documentos). Estos enlaces integran una gama de información de diversas categorías, que puede contener desde un simple texto hasta imágenes, video, sonidos, etc.

El funcionamiento de la World Wide Web (www) está vinculado estrechamente al uso de páginas web y del hipertexto.

- Páginas web

Son lugares donde se visualiza la información. Han sido diseñados de una forma accesible, para que el usuario pueda leer su contenido fácilmente. Están instaladas en servidores web, que son computadoras conectadas directamente a Internet y que permiten a los usuarios acceder a una gama de recursos.

- HTTP *(Hypertext Transfer Protocol)*

Es el protocolo de transferencia de hipertexto, utilizado por la *World Wide Web*. El HTTP define la manera en que los mensajes son enviados y reciben un formato, y qué acciones deben tomar los servidores de web o los navegadores en respuesta a los comandos. Los documentos de hipertexto se pueden encontrar entrelazados mediante palabras o símbolos. Cuando en el texto aparece una nueva palabra o un nuevo concepto, el hipertexto hace posible dirigirse a un documento que ofrezca más detalles sobre el tema. Suele

aparecer señalado con un subrayado o con color azul. Al colocar sobre él el apuntador del *mouse* se activa un cambio.

- **Navegadores**

Para tener acceso a las páginas web es necesario contar con un *software* que permita facilitar este trabajo. Se trata de los navegadores (*browsers*). Los más utilizados son Netscape Navigator e Internet Explorer. Además, mediante los navegadores se puede acceder a otros servicios, como correo electrónico o listas de interés. Se les conoce también como puntos de inicio (*start points*); es decir, un conjunto de enlaces que nos ubican en determinados temas.

- **Portales o buscadores**

Los portales son una especie de motores de búsqueda, pero que contienen información específica para usuarios determinados. En otras palabras, enfocan su contenido a regiones o países, o bien clasifican a sus usuarios por profesiones o gustos. El aumento de la información en Internet es una de las razones de su surgimiento, y la comercialización regional ha permitido su incorporación.[8]

- **Correo electrónico (*e-mail*)**

El correo electrónico o *e-mail* (abreviatura de *electronic mail*) es una de las aplicaciones más utilizadas e importantes de Internet. Se usa como un valioso recurso de comunicación, por medio del cual cada día millones de mensajes son enviados a algún lugar del mundo y llegan a su destino en minutos o segundos.

El correo electrónico se utiliza para transferir en forma sencilla y económica todo tipo de información, como textos, gráficos, videos, sonido, *software*, etc. Incluso se puede enviar archivos anexos (*attachments*). Basta con conocer la dirección electrónica del destinatario.

---

[8] Ejemplos de portales son el Portal Tributario de SUNAT (<http://www.sunat.gob.pe/>), el Portal Peruano de las Tecnologías de la Información (<http://www.partalti.com>), el Portal Jurídico Asesor (<http://www.asesor.com.pe>), <http://www.yahoo.com> y <http://www.google.com>.

Para usarlo es necesario estar conectado a Internet y contar con un programa de administración de correo, como Outlook de Microsoft. Otra alternativa es tener una cuenta de correo en un servidor destinado para ello, como Hotmail, Yupi o Yahoo. Estos últimos se pueden utilizar en forma gratuita. Sin embargo, es recomendable leer siempre las políticas de privacidad con que cuentan, que son los términos en los que se presta el servicio de correo.

El *e-mail* fue concebido para que tuviera el mayor parecido posible con el correo convencional o postal, a fin de que se pudiera usar con la misma facilidad pero con un importante ahorro de tiempo. El usuario debe de contar con una dirección personal para recibir la correspondencia. Esta dirección electrónica permite que los mensajes lleguen a su destino sin importar el lugar donde el usuario se encuentre y, en algunos casos, le permite leerla desde cualquier computadora.

Entre sus ventajas están la rapidez en el envío y en la recepción de mensajes, la comodidad de poder verificar la correspondencia electrónica en cualquier momento y el ahorro que implica, tanto en tiempo como en estampillas, postales, papel, etc. Además, recordemos que podemos mandar un mismo mensaje a muchos destinatarios a la vez e incluso confirmar si lo han recibido.

- **Telnet**

Este servicio permite acceder a una computadora en forma remota, de manera que el usuario pueda controlarla aunque esté a kilómetros de distancia. Para usar Telnet es necesario contar con la autorización de la computadora, ya que está protegida por claves de acceso y sistemas de seguridad para evitar accesos no autorizados. Actualmente este servicio es utilizado principalmente por los administradores de redes, quienes ingresan en forma remota a los servidores que tienen a su cargo para realizar cambios sin necesidad de estar físicamente cerca.

- **FTP (Protocolo de Transferencia de Archivos o *File Transfer Protocol*)**

Es una versión reducida de Telnet. Sirve para transferir archivos de una computadora a otra, de una manera rápida y eficaz. Por lo

general se utiliza para actualizar las páginas web instaladas en servidores de uso público y que, mediante una clave de autorización, permiten al usuario enviar actualizaciones de la información que contiene su sitio, como archivos, datos e imágenes, entre otros.

- **Videoconferencia**

Se trata de un sistema que permite mantener comunicaciones con imagen y sonido en tiempo real entre dos o más personas que se encuentran en lugares distintos. Los interlocutores pueden verse y hablarse como si estuvieran en la misma sala de reuniones. Esta utilidad hace posible, entre otras cosas, intercambiar datos, información, gráficos o diapositivas.

1.5. Cómo conectarse a Internet

Para que un usuario pueda conectarse a Internet es preciso que cuente con el equipo necesario, que se detalla a continuación.

1.5.1. Computadora

Conocida también como computadora personal o PC (*personal computer*). Esta requiere una configuración mínima necesaria para una navegación aceptable.

1.5.2. Hardware *de acceso*

Hay varias formas de conectar la computadora a Internet. La más común es la utilización de un módem, aunque existen otras opciones.

- **Acceso telefónico con módem (modulador y demodulador)**

Es la forma más sencilla de acceder a Internet. El módem, que puede ser una tarjeta interna o un dispositivo periférico (externo), convierte las señales de información binarias de una computadora en señales análogas o digitales y viceversa, es decir, convierte la señal enviada por cable telefónico en lenguaje de computadora.

- **Acceso telefónico o ISDN (*Integrated Services Digital Network*)**

La RDSI (Red Digital de Servicios Integrados) es una conexión que utiliza la infraestructura de cable telefónico usando un estándar de

transmisión digital mediante un adaptador ISDN. Este transporta la información de una manera directa, es decir, en el mismo lenguaje de computadora, por lo que no es necesario usar un módem. Este tipo de conexión tiene una mayor velocidad de acceso y un menor costo.

Existen otras formas de conectarse a Internet para prestar algún servicio específico, como ser proveedor de servicios de Internet o tener un enlace dedicado. El costo de estas conexiones es mucho mayor. Además, existe la telefonía inalámbrica, que permite al usuario tener acceso por vía telefónica a la información que ha programado.

1.5.3. Software *de navegación*

Son los programas que es preciso instalar en la computadora para que tenga acceso a Internet. Son dos: el programa de acceso y el navegador.

- Programa de acceso

Es proporcionado de manera directa por el proveedor de servicios de Internet. Contiene los datos técnicos del servidor al que se conectará, como el número de acceso o la configuración del POP.

- Navegador o *browser*

Es el programa que permite ver y explorar la información en Internet. Los navegadores han evolucionado y proporcionan un ambiente amigable para el usuario. Los más utilizados son Netscape y el Internet Explorer de Windows. Funcionan independientemente del sistema operativo de la computadora.

1.5.4. Acceso a Internet

Para acceder a Internet hay dos opciones: recurrir a una conexión directa o a un proveedor de servicios de Internet (PSI). La primera es muy onerosa y está destinada generalmente a empresas, gobiernos o instituciones que necesitan un servicio dedicado, proporcionado en la mayoría de los casos por un PSI. Para obtenerla es necesario llenar una lista extensa de requisitos.

La segunda opción, la más utilizada en el medio, es tener acceso a Internet por medio de un PSI, con el cual se celebra un contrato de proveedor de acceso a Internet. El costo de este acceso dependerá

de factores como el servicio con el que se quiera contar, las horas mensuales de navegación y la velocidad deseada. Lo más común es el acceso telefónico, es decir, entrar a Internet usando la infraestructura de comunicación telefónica.

1.6. Implicancias jurídicas del empleo de Internet

Como hemos señalado, el empleo de Internet trae una serie de consecuencias en el ámbito jurídico, en lo que concierne al tratamiento de nuevas formas de realización de actos jurídicos.

Dentro del derecho mercantil —rama del Derecho a la que pertenece el comercio electrónico— y de acuerdo con lo afirmado por Jordi Blasco,[9] los principales problemas jurídicos son los siguientes:

1.6.1. Nombres de dominio e infracciones de marcas registradas

El uso y la propiedad de una palabra determinada como marca y como dominio por dos personas u organizaciones distintas ha provocado uno de los conflictos más comunes y candentes derivados de la utilización de Internet. También surgen conflictos del uso, por parte de un dominio, de una palabra muy similar a la denominación de una marca.

Los diferentes procedimientos y garantías para la adquisición y conservación de una marca y de un dominio han obligado a muchas compañías (y también a algunos particulares famosos) a renunciar a utilizar sus signos de identidad o a entablar diversos pleitos para poder ser identificados en la red del mismo modo que en la realidad. Estamos hablando del *cybersquatting* o *ciberokupación*.

De la misma manera, la eficacia de la protección del registro de una marca disminuye cuando la marca es registrada como nombre de dominio en otro país.

---

[9] BLASCO, Jordi. «Problemas jurídicos derivados del uso de Internet». En <www.derecho.com/boletin/articulos/articulo0035.htm>.

1.6.2. Infracción de derechos de propiedad intelectual o industrial

Las copias ilegales de programas y de obras protegidas en general (ya sean música, imagen o simplemente texto) y su fácil distribución en Internet son dos de los problemas legales que más cobertura tienen en los medios de comunicación.

En nuestro país la infracción de los derechos de autor es tan común que es normal adquirir un programa de computación pirata «a la carta». Lo mismo sucede en el caso de la música.

1.6.3. Competencia desleal

Las empresas de alta tecnología e Internet son muy sensibles a los problemas derivados de la vulneración de secretos empresariales. Muchas veces sus únicos activos realmente valiosos son intangibles. La vía más habitual, aunque irregular, de hacerse de los secretos de negocio y del *know-how* de la competencia es la contratación de parte de su personal altamente calificado.

Igualmente, es cada vez más frecuente la difusión por Internet de informaciones falsas o deliberadamente distorsionadas, que persiguen el descrédito de las empresas competidoras.

1.6.4. Defensa de la competencia

La creación de mercados B2B (*business to business*)[10] puede ser una solución para optimizar la transferencia de recursos y de información entre diversas partes de los mercados y de la cadena de valor. La posibilidad de saltarse eslabones intermedios en la cadena de distribución es muy atractiva. La existencia de Internet permite suponer que pueden eliminarse intermediarios entre los productores y los consumidores, sean estos finales o no.

Sin embargo, también existen casos de sedes B2B o de *marketplaces* sectoriales, controlados por grandes multinacionales, que

[10] El B2B es un nivel de comercio electrónico que será desarrollado en el siguiente punto.

han sido acusados de replicar la situación existente en el mercado «real» o tradicional (donde hay casos de monopolio, oligopolio y control de precios del mercado, entre otros). Estas iniciativas B2B se convierten así en un nuevo canal de distribución, aunque tienen los mismos dominantes y dominados, y, sobre todo, una fijación de precios poco o nada transparente.

Además, las expectativas enormes de negocios que se han generado alrededor de Internet han provocado que grandes corporaciones intenten controlar de forma monopolística el mercado o partes de él. Quizás el ejemplo más conocido sea el de Microsoft, por la atención que le han dedicado las autoridades defensoras de la libre competencia.

1.6.5. Fraudes cometidos en la red

Entre muchos otros, podemos citar como ejemplos de fraude los siguientes:

- Abuso de las tarjetas de crédito: cargos no autorizados y venta de datos confidenciales.
- Creación de estructuras piramidales de venta, en las que el beneficio básico se consigue mediante la compra de productos que necesariamente deben hacer los nuevos «afiliados» al sistema o empresa.
- Ventas en la web de toda clase de productos, que exigen un pago por adelantado sin que se entregue el producto comprado.
- Difusión de informaciones falsas por Internet, que originan, por ejemplo, caídas en la cotización de las acciones de la compañía afectada por la información manipulada y que sirven a algunos para comprar o vender títulos en mejores condiciones.

1.6.6. Conflictos de jurisdicción

Un sistema global y abierto como Internet lleva implícita la relación entre personas que pueden encontrarse a miles de kilómetros y estar sujetas a leyes muy distintas. ¿Qué pasa si tenemos algún

conflicto legal con alguna de ellas? ¿En qué país plantearemos el reclamo? ¿Cuáles son los tribunales competentes?

Esta discusión no está cerrada. En la práctica presenta muchos problemas y nada indica que vayan a desaparecer en el corto plazo. En general, los conflictos de jurisdicción surgen como consecuencia de operaciones comerciales fallidas (conflictos por la calidad de lo comprado, por los pagos realizados con ocasión de una compra, por la autorización para vender por Internet mercancías prohibidas en el territorio del comprador, etc.). También aparecen conflictos por agresiones de un tercero (intromisión en sistemas ajenos, fraudes informáticos o casos de difamación, por ejemplo).

1.6.7. Comercio electrónico

La problemática jurídica que resulta del empleo de Internet para el desarrollo del comercio electrónico será analizada en el siguiente punto. Los principales problemas son la identidad de los sujetos, la integridad y la confidencialidad de los mensajes, los medios de pago y el valor probatorio de los documentos electrónicos.

2. COMERCIO ELECTRÓNICO

2.1. Reseña histórica

El comercio electrónico, como intercambio electrónico de datos (IED), se originó en los Estados Unidos en los años 60 con iniciativas independientes en los sectores del ferrocarril, negocios al detal, verdulerías y fábricas de automóviles; y fue diseñado para fortalecer la calidad de los datos que ellos estaban intercambiando con otros en la cadena de proveedores y usándolo para sus procesos internos. En los 70's la transferencia electrónica de fondos (TEF) a través de redes de seguridad privadas dentro de las instituciones financieras expandió el uso de las tecnologías de telecomunicación para propósitos comerciales, permitiendo el desarrollo del intercambio computador a computador de la información operacional comercial en el área financiera, específicamente la transferencia de giros y pagos. El IED usa documentos electrónicos con formato estándar que reemplazan los documentos comerciales comunes, tales como, facturas, conocimientos de embarque, órdenes de

compra, cambios en órdenes de compra, requerimientos de cotizaciones y recepción de avisos —los 6 tipos más comunes de documentos comerciales que constituyen el 85% de las transacciones comerciales oficiales en los Estados Unidos—.[11]

2.2. Definición

A continuación citamos diversas definiciones de comercio electrónico.

> Intercambio telemático de información entre empresas (*business to business*) o entre empresas y consumidores (*business to consumer*) que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles (datos, documentos, imágenes, música, videos, servicios, etc.) o en un pedido electrónico de bienes tangibles. Ampliamente, se ha dicho que es el conjunto de actividades con finalidad mercantil que se realizan mediante sistemas y redes computacionales, sin que exista contacto físico directo entre quien oferta un bien o un servicio y quien lo demanda, y que cubre no solamente actos comerciales directos sino también acciones preparatorias como las de publicidad y mercadeo.[12]

Esta definición nos parece importante, puesto que resalta el ámbito en el que opera el *e-commerce*. Este no se limita a los actos de comercio directos —es decir, a la compra de bienes o servicios—, sino que además se aplica a las fases de preventa y postventa.

> El comercio electrónico se puede entender como cualquier forma de transacción o intercambio de información basada en la transmisión de datos sobre redes de comunicación como Internet. El concepto de comercio electrónico no sólo incluye así a la compra y venta electrónica de bienes, información o servicios, sino también al uso de la Red para actividades anteriores o posteriores a la venta.[13]

---

[11] «Qué es comercio electrónico». En <http://ute.edu.ec/~mjativa/ce/que-es-com-elec.html>.

[12] JIJENA LEIVA, Renato Javier. «Comercio electrónico, Estado y Derecho». *Ponencias VII Congreso Iberoamericano de Derecho e Informática*. Lima, 2000, p. 233.

[13] JUEZ MARTEL, Pedro. «El comercio electrónico: ¿Hacia una nueva revolución económica y jurídica?». *Ponencias VII Congreso Iberoamericano de Derecho e Informática*. Lima, 2000, p. 352.

Esta definición es también importante, ya que resalta el medio tecnológico que caracteriza toda operación de comercio electrónico.

Citamos la siguiente definición que, consideramos, no tiene carácter restringido:

> [...] todas las transacciones de valor que involucren la transferencia de información, productos, servicios o pagos por medio de redes electrónicas. [...] El comercio electrónico [...] se refiere generalmente a todas las formas de transacciones relacionadas con las actividades comerciales, incluyendo organizaciones e individuos, que están basadas en el proceso y transmisión de datos digitalizados, incluyendo texto, sonido e imagen.[14]

La Comisión de la Unión Europea en la comunicación COM.97.157 define el comercio electrónico como

> [...] el desarrollo de actividad comercial y de transacción por vía electrónica y comprende actividades diversas: la comercialización de bienes y servicios por la vía electrónica; la distribución *on line* de contenido digital; la realización por vía electrónica de operaciones financieras y de bolsa; la obra pública por vía electrónica y todo procedimiento de ese tipo elaborado por la Administración Pública.

A continuación proponemos la siguiente definición: el comercio electrónico, o *e-commerce*, es el conjunto de relaciones comerciales que se entablan por cualquier tipo de personas mediante soportes electrónicos.

Esta definición contiene los elementos básicos del comercio electrónico. En primer lugar, hace referencia al tipo de relaciones comprendidas, es decir, cualquier tipo de relación comercial, desde una oferta publicitaria hasta la ejecución de un contrato de compraventa en línea. Esto es, abarca las fases de preventa, venta y postventa de bienes y servicios.

---

[14] «Qué es comercio electrónico». En <http://ute.edu.ec/~mjativa/ce/que-es-com-elec.html>.

En segundo lugar, no hace una referencia taxativa a los sujetos que intervienen en estas relaciones, ya que pueden darse entre consumidores, empresas e incluso el Estado, en todas las combinaciones posibles. En otras palabras, es una definición abierta respecto de los sujetos, sin encuadrarlos dentro de categorías determinadas.

Por último, la definición indica el medio por el cual se entablan estas relaciones comerciales. El concepto de soporte electrónico es amplio; no se restringe únicamente a Internet, que es el medio por excelencia, pues existen distintos soportes electrónicos como el EDI (*Electronic Data Interchange*). Además, es posible que aparezcan nuevos soportes tecnológicos que estarían incluidos en el concepto de comercio electrónico. Por esta razón, nuestra definición es abierta también en cuanto a la tecnología empleada.

2.3. Características

De acuerdo con la definición propuesta, el comercio electrónico tiene las siguientes características:

2.3.1. Medio de comercio electrónico de trascendencia económica

Como afirma Francisco González:

> En el comercio electrónico hay algo más que el medio de intercambio usado. Esta forma de comercio va emparejada inseparablemente con la economía contemporánea, caracterizada por la globalización de los intercambios, el constante crecimiento de las capacidades de los productores y de las necesidades y exigencias de los clientes. El comercio electrónico introduce cambios en el contacto entre las empresas, entre cliente y empresa, y entre la empresa y sus trabajadores. Está claro que no es una simple novedad tecnológica; va a revolucionar la economía. La pregunta es si esta forma de comercio sustituirá a cualquier otra forma de comercio.[15]

[15] GONZÁLEZ GALLEGO, Francisco. «Confianza y fidelización en el comercio electrónico». En <http://www.tel.uva.es/~fgongal/ce/trabajo/critica.htm>.

El comercio electrónico entra en desarrollo en una etapa en la cual la eficiencia en la prestación de bienes y servicios con valor agregado es la que determinará la supervivencia entre competidores. El *e-commerce* es una herramienta muy valiosa para lograrlo.

2.3.2. Medio de comercio virtual

Los sujetos que intervienen en una operación de comercio electrónico no tienen una proximidad física que les permita entablar una relación inmediata, a diferencia de lo que sucede en el comercio tradicional, en el cual los sujetos tienen la posibilidad de conocerse físicamente. Los sujetos que participan en el comercio electrónico pueden encontrarse en distintos países, hecho que hace imposible que exista un contacto físico que les permita verificar la existencia del otro.

Es evidente la ventaja del comercio electrónico, pues no requiere de la proximidad física de los sujetos participantes. Por el contrario, la proximidad es indiferente. De esta manera, será incluso lo común que los sujetos se hallen en lugares distintos.

Por este motivo, el *e-commerce* es un medio de comercio virtual, ya que los sujetos participantes interactúan en un espacio y en un medio que no es físicamente perceptible.

2.3.3. Medio de comercio de vocación universal

Al ser Internet el soporte tecnológico del comercio electrónico, y ya que, como hemos señalado, es una red abierta a la cual solo se puede tener acceso si se cuenta con la tecnología adecuada, el comercio electrónico podrá ser llevado a cabo por cualquier persona que tenga la posibilidad de conectarse a Internet. Es evidente la vocación de universalidad del *e-commerce*, pues no se ve limitado por barreras geográficas estatales o de cualquier otro tipo, salvo las económicas o culturales.

2.3.4. Vinculación tecnológica

El comercio electrónico es, por su propia naturaleza, un medio de comercio que requiere necesariamente de la tecnología adecuada

para su desarrollo. Por este motivo su dependencia de la tecnología es vital, a diferencia de lo que ocurre en el comercio tradicional, en el cual no es imprescindible contar con tecnología muy sofisticada.

Por esta razón, para comprender la naturaleza de esta actividad es necesario conocer el funcionamiento de la tecnología detrás de Internet. Solo así será posible comprender cabalmente sus implicancias jurídicas, saber cuáles son sus limitaciones y su problemática y proponer alternativas de solución.

2.3.5. Medio de comercio de bajos costos

El comercio electrónico reduce los costos de transacción, ya que centraliza la oferta y la demanda de bienes y servicios. De la misma manera contribuye con la reducción de costos administrativos e impositivos, puesto que reduce el proceso de distribución e intermediación. Esta característica, que es una ventaja, se puede apreciar en el cuadro de evaluación de costos de la página 30.

2.3.6. Medio de comercio rápido

Una de las ventajas principales del comercio electrónico es la rapidez con la que se puede llevar a cabo una transacción de comercio, a diferencia de lo que sucede en el comercio tradicional. Es un medio que agiliza el tráfico patrimonial, posibilidad que trae como consecuencia el aumento de las transacciones comerciales.

2.4. Elementos integrantes del comercio electrónico

Según las definiciones mencionadas en el apartado 2.2, hay tres elementos principales en el comercio electrónico: los sujetos, los actos de comercio celebrados por los sujetos y la infraestructura de comercio electrónico.

2.4.1. Los sujetos

No existe limitación alguna en cuanto a los sujetos participantes en las relaciones comerciales por medios electrónicos, como se puede ver en nuestra definición propuesta. Sin embargo, para efectos de

mera clasificación, existen tres categorías de sujetos en el comercio electrónico: *consumers* o consumidores, *business* o empresa y *government* o Gobierno.

Consumers o consumidores: son las personas que tienen la posición de demandantes en un mercado determinado. Pueden ser personas naturales o jurídicas. Existen ciertas dudas respecto de considerar a las personas jurídicas como consumidores, puesto que por su propia naturaleza todas las actividades que realicen dentro de su objeto social son consideradas actos empresariales, característica que las incluiría en la categoría *business*. Sin embargo, pensamos que ciertos actos de comercio realizados por personas jurídicas pueden ser considerados actos de consumidores.[16]

Business o empresa: son las personas que ofertan bienes o servicios en un mercado determinado. Generalmente son personas jurídicas; sin embargo, las personas naturales pueden estar incluidas dentro de esta categoría.[17]

Government o Gobierno: se trata del Estado en los casos en que actúa como un agente económico. En la actualidad, se limita la actuación del Estado a la de un mero agente regulador en la economía. No obstante, existen excepciones. Tanto es así que muchas convocatorias a concursos públicos se realizan por Internet, mediante páginas web estatales.

2.4.2. Los actos de comercio propiamente dichos

Los actos de comercio, según nuestra definición, pueden ser de cualquier naturaleza, sin limitación alguna, excluyendo limitaciones tales como orden público o buenas costumbres. Es en este

[16] Es el caso, por ejemplo, de la contratación de un servicio de bufé para la celebración de año nuevo o del aniversario de la empresa.

[17] Un ejemplo en el cual las personas naturales actúan como *business* es el de los vendedores de bienes usados, que se alojan en las páginas web de proveedores. Un ejemplo es la página de la tienda virtual Amazon.com, en la cual personas naturales tienen la posibilidad de ofertar bienes usados.

punto en el que se encara una de las dificultades jurídicas del comercio electrónico. ¿Cuál ley determinará las buenas costumbres? ¿La ley del país del vendedor, del comprador o del lugar donde se encuentra alojada la página web del vendedor? Se trata del problema de la ley aplicable.

2.4.3. La infraestructura de comercio electrónico

Están comprendidos en la infraestructura de comercio electrónico tanto el soporte tecnológico que lo hace posible como la existencia de las entidades que participan en él.

En cuanto al soporte tecnológico, se hace referencia directa pero no exclusiva a Internet. No solo se debe considerar soporte tecnológico la computadora y sus programas (*software* y *hardware*) sino también, el sistema de línea telefónica que permite la conexión de un ordenador en la red.

Dentro de las entidades que forman parte de la infraestructura del comercio electrónico se encuentran los proveedores de servicio de Internet, de los cuales ya nos hemos ocupado, y las entidades de certificación o terceras partes de confianza,[18] a las cuales nos referiremos con mayor profundidad en el siguiente capítulo. Sin embargo, consideramos pertinente precisar que las entidades de certificación no deben ser consideradas sujetos en el comercio electrónico sino parte de la infraestructura necesaria. Esta precisión se debe a que los sujetos del *e-commerce* se valen de estas entidades para la realización de los actos de comercio electrónico.

2.5. Niveles en el comercio electrónico

Los niveles de comercio electrónico están determinados por los sujetos entre los cuales se entablan las relaciones de comercio. Existen cinco niveles:

---

[18] La finalidad de estas entidades es certificar la identidad de los sujetos que intervienen en una relación comercial llevada a cabo por medio de Internet.

2.5.1. Business to business

El *business to business* (B2B) comprende las relaciones entre dos o más empresas. En su forma más simple es el mecanismo de compras interempresariales usando medios electrónicos (Internet, EDI).

Los medios con los cuales se entablan estas relaciones han sido diversos. El más conocido antes del apogeo del Internet fue EDI,[19] un mecanismo de compras interempresariales con medios electrónicos. Se trataba de una red de carácter cerrado, a diferencia de Internet. Su limitación se hace evidente en el hecho de que solo podían relacionarse con este medio las empresas que estuvieran dentro de la red cerrada.

El B2B es la fuerza y el motor del comercio electrónico mundial por su potencial de ahorro de costos para las empresas. Se puede definir tres categorías en el B2B:

- *Vertical* marketplaces

Facilitan el comercio o proveen servicios a los miembros de una industria. Los sectores en los cuales se han desarrollado *marketplaces* son la electrónica, la industria química, la energía, la alimentación, la fabricación de instrumentos de precisión, el acero, la industria automotriz y servicios, entre otros.

- *Horizontal* marketplaces

Ofrecen servicios que ligan a distintas industrias, es decir, proveen la plataforma en la que ofertantes y demandantes de diversas industrias (por ejemplo, las empresas de proveedores de productos de oficina) se encuentran para intercambiar productos y servicios.

- Facilitadores del *marketplace*

Para que los intercambios electrónicos se desarrollen en los *marketplaces* se requieren muchas aplicaciones, que son proporcionadas por empresas tecnológicas.

---

[19] GALLEGOS, Hugo. «Ciclo de conferencias Comercio Electrónico: Fundamentos y Experiencias». 14 -16 de agosto, 2000. Lima: Pontificia Universidad Católica del Perú.

2.5.2. Business to consumer

El nivel *business to consumer* (B2C) está constituido por las relaciones entre las empresas y sus clientes en forma singular y a pequeña escala. En esta característica se diferencia del B2B, que es un medio a gran escala, es decir, al por mayor.

Con respecto a los consumidores, este nivel presenta ventajas y desventajas.

Ventajas

- Los compradores obtienen nuevos servicios de valor añadido sobre la oferta tradicional.
- Los compradores no tienen que desplazarse, hecho que implica un ahorro de tiempo y dinero.
- Es un medio interactivo que permite obtener información y comparar prestaciones y servicios fácilmente.

Desventajas

- Hay problemas de seguridad y de privacidad en cuanto a los datos que son transmitidos en la red. Ahondaremos en este tema en el punto concerniente a las implicancias jurídicas del comercio electrónico.
- Existen problemas de comunicaciones, que pueden deberse a fallas tecnológicas.
- La virtualidad del medio también puede convertirse en un problema. No es posible tocar los productos. Existen las llamadas *tiendas virtuales,* en las cuales se exhiben los productos, con lo que surgen los mismos inconvenientes de una venta sobre catálogo.

Con respecto a las empresas, este nivel presenta las siguientes ventajas y desventajas.

Ventajas

- Permite acceder a nuevos mercados y negocios debido al carácter abierto de la red, que no conoce fronteras geográficas ni estatales.

- Supone un nuevo canal de comunicación que permite dirigirse a los clientes de forma personalizada.
- Es una fuente de información. Cada vez que una persona accede a una página web, el vendedor que pone la página a disposición de los internautas[20] tiene acceso a información sobre las preferencias de los potenciales consumidores. Por ejemplo, el tipo de consumidores que visitan la página y la periodicidad con que la visitan, entre otros datos comerciales de importancia para el vendedor.
- Se disminuye la diferencia entre las empresas. En otras palabras, cualquier empresa, sea grande o pequeña, puede entrar en el mercado internacional y ofertar sus productos como cualquier *business* del mundo. De esta manera, se hace evidente que en el mercado electrónico la eficiencia, y no el tamaño, es uno de los puntos centrales para garantizar una efectiva competencia.

Desventajas

- Es necesario un ajuste de la empresa a la red. Un cambio de mentalidad es obligatorio. En efecto, el comercio electrónico no es únicamente el empleo de una nueva tecnología. Además, es la adaptación de nuestra concepción del comercio a los nuevos usos y costumbres comerciales.
- Se debe hacer una inversión y un esfuerzo en los cambios de estrategia. Como hemos señalado, el acceso a Internet está únicamente supeditado a la posesión de la tecnología adecuada. Este hecho representa un costo de inversión relativamente alto con respecto a los beneficios que la tecnología lleva consigo y puede hacer que la inversión sea descartada.
- La infraestructura tecnológica está en constante evolución. La tecnología evoluciona al punto de que se puede considerar que una computadora adquirida hace tres meses está desactualizada. En efecto, la tecnología se perfecciona

[20] Se llama *internautas* a los usuarios de Internet.

constantemente y, con ella, las formas de realizar comercio. Es muy difícil y costoso estar constantemente actualizado con las nuevas formas de comercio, y eso acarrea que estas nuevas formas puedan ser dejadas a un lado.

Consideramos que los dos niveles mencionados, el B2B y el B2C, son los de mayor importancia en la actualidad. A continuación señalamos ciertas diferencias entre ambas modalidades, a fin de establecer con mayor precisión los alcances de cada nivel.

Diferencias entre el B2C y el B2B

Rubro	B2C	B2B
Costo de conexión	Bajo con múltiples ofertantes.	Alto cuando pocos ofertantes calificados están integrados a la *e-frastructure*[21]
Tipo de relación	Directa	Previa negociación
Tipo de transacción[22]	En promedio, precios un poco más bajos.	En promedio, precios mucho más altos.
Modelo de ingresos	El volumen del tráfico es crítico. Los grandes compradores son lo más importante.	No necesita de cada consumidor. Solo necesita tener a los clientes correctos.

2.5.3. Consumer to consumer

Es posible que entre consumidores se entablen relaciones comerciales, a las que se denomina *consumer to consumer* (C2C). Por supuesto, este tipo de relación no se da usualmente ni con la frecuencia del B2B o del B2C. Sin embargo, no sería conveniente excluir del comercio electrónico a este nivel.

[21] E-Frastucture es el *software* que tiene por objeto facilitar el manejo de contenidos y facilitar el comercio basado en tecnología web.

[22] En el B2C los tipos de transacciones suelen ser más bajos porque generalmente son transacciones a pequeña escala. En el B2B, en cambio, las transacciones generalmente son a gran escala.

2.5.4. Business to government

En el nivel *business to government* (B2G), se desenvuelven las relaciones entre las empresas y el Estado. Los *business* en este caso serán los proveedores de bienes o servicios.

2.6. Fases en una transacción de comercio electrónico

Las etapas en las cuales se desarrolla una operación de comercio electrónico son las mismas que las de una operación de comercio tradicional o, en todo caso, similares. La diferencia radica en los medios de los cuales los sujetos participantes se valen para interactuar y tener relaciones comerciales.

2.6.1. Localización o identificación de las partes, o fase de preventa

Esta es la etapa inicial. En ella, la parte que demanda un bien o servicio determinado lo busca de acuerdo con sus requerimientos, mientras que la parte que oferta un bien o servicio ubica un mercado en el cual introducirlo. Ambas partes interactúan en el mercado con el objeto de satisfacer sus necesidades, sea por primera vez o no. En la medida en que la parte demandante u ofertante ubique a su contraparte, estas necesidades estarán satisfechas.

Por este motivo, esta etapa es llamada *localización de las partes*. Cada parte, a fin de satisfacer sus necesidades, localiza a su contraparte. La particularidad en el comercio electrónico es que este proceso de localización se lleva a cabo principalmente con medios electrónicos.

De esta manera, la parte ofertante de un determinado bien o servicio se valdrá de Internet para lograr este objetivo, y la parte demandante explorará en la red las ofertas que más le atraigan.

La participación del Derecho en esta etapa se da en el área de publicidad y protección al consumidor. Es necesario que se garantice una publicidad apropiada de los bienes y servicios que se oferten en la red. A diferencia de lo que sucede en una transacción

tradicional, en la cual el posible comprador tiene la posibilidad de tener físicamente los productos o servicios que adquirirá, en Internet no es posible tener esa proximidad física. Por lo tanto, la única manera de conocer las características del bien o servicio a adquirir es la descripción que realice el vendedor u ofertante. Se trata de una fase de preventa, de publicidad, de promoción de bienes o servicios.

2.6.2. Contratación electrónica

Una vez producida la localización de las partes, estas consolidan su vinculación mediante la contratación, para lo cual se valen de medios electrónicos como Internet.

En esta etapa tiene su actuación el *e-frastucture*. No solo participa Internet sino, también, los medios de seguridad para las transacciones comerciales, como la firma digital, los certificados digitales y las entidades de certificación. La existencia de estos medios de seguridad en el comercio y su permanente desarrollo son necesarios para la realización del comercio electrónico. En efecto, como explicaremos, uno de los inconvenientes de esta actividad es la inseguridad latente con respecto a la integridad de la información y la identidad de las partes contratantes.

De igual manera, en esta fase, la participación del Estado es básica. En efecto, es esencial que adapte su legislación para que los sistemas electrónicos como Internet sean considerados medios para la contratación. Un ejemplo de esta adaptación en el Perú es el caso de la ley de firmas y certificados digitales, así como la modificación del Código Civil en lo referente a los medios para contratar y el reconocimiento de la firma digital.

2.6.3. Ejecución y conclusión de los contratos

Esta es la última etapa de una operación comercial y supone que las partes se han obligado válidamente usando medios electrónicos.

En esta fase, las partes vinculadas deberán ejecutar las prestaciones a las cuales se han obligado. En el caso del comprador, deberá cumplir con el pago del bien o servicio que adquiera. Generalmente,

en las operaciones de comercio electrónico el pago es la primera prestación que se cumple, inmediatamente después de la celebración del contrato. En el caso del vendedor, deberá cumplir con prestar el servicio o entregar el bien adquirido. El medio para hacerlo dependerá del bien que es objeto de la transacción.[23]

Cobran importancia en esta etapa, en primer lugar, los medios de pago electrónicos, mediante los cuales el comprador cumplirá con la ejecución de su prestación. Ejemplos de medios de pago son el monedero electrónico y la tarjeta de débito. Debido a que existe la posibilidad constante de un eventual incumplimiento de cualquiera de las prestaciones a las cuales se obligan las partes, será necesario el establecimiento de un sistema de heterocomposición de los posibles conflictos. En este sistema será necesario precisar, entre otros aspectos, la ley y la jurisdicción aplicables, así como la validez probatoria de los documentos electrónicos.

Por último, en esta etapa, la intervención no solo del Estado en particular sino de la comunidad de Estados en general consistirá en determinar las normas aplicables para la uniformidad de los medios de pago en el comercio electrónico, las políticas de importación de productos y servicios, y el pago o exoneración de derechos arancelarios, entre otros aspectos.

2.7. El comercio electrónico a luz de la ley modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional

Consideramos necesario hacer una breve descripción de la ley modelo sobre comercio electrónico, que tiene por objeto publicitar y adaptar los conceptos básicos en el *e-commerce*.

---

[23] Por ejemplo, en el caso de la compra por Internet de una pizza entregada a domicilio, el vendedor requerirá de un sistema de entrega de pizzas (*delivery*) adecuado para cumplir la entrega en las condiciones pactadas. En el caso de la venta de un *software*, el sistema de entrega será el medio electrónico mediante el cual se entregará el bien.

El artículo primero de la ley modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) para el comercio electrónico (en adelante la ley modelo) define su ámbito de aplicación en los términos siguientes: «La presente ley será aplicable a todo tipo de información en formas de mensaje de datos utilizada en el contexto de actividades comerciales».

La norma establece que por mensajes de datos se entiende la información generada, enviada, recibida, archivada o comunicada por medios electrónicos, ópticos o similares, como el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax, entre otros.

Por EDI, la ley modelo entiende la transmisión electrónica de información de una computadora a otra. Para que exista, la información debe tener una estructura adecuada a las normas técnicas vigentes. Por último, la norma contempla la existencia de tres sujetos participantes en el comercio electrónico. El iniciador de un mensaje de datos es quien, como figura en el mensaje, haya actuado por su cuenta o en cuyo nombre se actúa para enviar o generar el mensaje antes de ser archivado. El destinatario es la persona designada por el iniciador para recibir el mensaje, siempre y cuando no esté actuando a título de intermediario. Finalmente, el intermediario es el individuo que actúa por cuenta de otro para enviar, recibir o archivar un mensaje, o que le presta algún otro servicio.

Se desprende de la norma que el concepto de *e-commerce* de la CNUDMI es todo intercambio de información por medios electrónicos con fines comerciales, definición que coincide con la nuestra.

2.8. Dificultades en el comercio electrónico

2.8.1. Dificultades financieras o económicas

Al tener este trabajo una orientación jurídica, no desarrollaremos a profundidad este tipo de dificultades. A continuación describiremos las principales.

- **Tecnología costosa**

Como hemos señalado, la puerta de acceso al comercio electrónico es Internet y, consecuentemente, también lo es la tecnología necesaria que hace posible su empleo. Si bien es cierto que en la actualidad el empleo de Internet se ha masificado, los costos para acceder a esta tecnología siguen siendo muy altos, sobre todo en países en vías de desarrollo como el Perú. Esto sin contar que la tecnología de seguridad para el *e-commerce* es aun más costosa.

Sin embargo, este obstáculo se está superando gracias a la existencia de las cabinas de Internet que han proliferado en los últimos dos años. En ellas, el costo de acceso a Internet se diluye entre los diferentes usuarios.

- **Preparación insuficiente**

La falta de formación adecuada sobre la tecnología de Internet y sus múltiples aplicaciones, como el *e-commerce*, ha restringido el empleo del Internet al uso del correo electrónico y del *chat*. De esta manera, se limita el potencial uso del Internet en el comercio electrónico. Asimismo, la falta de capacitación e información, tanto técnica como legal, trae como consecuencia la comisión de errores en la ejecución de operaciones de comercio.

Estos factores desalientan el empleo del comercio electrónico y producen inconvenientes en su ejecución.

- **Idioma predominante**

La tecnología de punta en materia de comercio electrónico ha sido desarrollada en los Estados Unidos. Por esta razón, el *software* y la tecnología han sido creados preponderantemente en inglés. Es el predominio de este idioma lo que dificulta el entendimiento y aprendizaje del funcionamiento del comercio electrónico. Actualmente, existen portales, como Yahoo, que cuentan con una versión en español. De la misma manera existen páginas latinoamericanas que realizan *e-commerce*, como <http://www.jungla.com>, que se dedica a la venta de libros.

No obstante, la participación de un usuario en el empleo de Internet será limitada en la medida en que no sepa inglés.

- **Infraestructura tecnológica en constante evolución**

Implica una constante capacitación y actualización tecnológica, con el correspondiente costo.

- **Políticas aduaneras**

Los obstáculos que representan las políticas aduaneras de los distintos Estados, así como los problemas de doble tributación, se convierten en dificultades jurídicas.

2.8.2. Dificultades jurídicas

Para explicar cuáles son las dificultades jurídicas del comercio electrónico, describiremos tres escenarios.

Imaginemos a un niño que tiene acceso a Internet desde su habitación, sin supervisión directa de sus padres. Una de las posibilidades que ofrece Internet es la agilización del comercio a distancia. El niño podría comprar desde su casa todos los juguetes de una lujosa tienda de su ciudad, efectuar un pedido de dos docenas de pizzas desde su casa u ofertar su casa en venta haciéndose pasar por su padre, con la intención de jugarles una broma de mal gusto tanto a sus padres como a sus eventuales contrapartes. La consecuencia de este «juego» será, en el mejor de los casos, que los padres tengan que pagar los juguetes o pizzas ordenados o, en el peor de los casos, que los padres ignorantes del juego de su niño se vean obligados a transferir su casa en condiciones muy perjudiciales.

Imaginemos al propietario de una modesta ferretería que ha decido incursionar en el mercado internacional al realizar una compra por Internet a un proveedor danés cuya página web encontró navegando. El proveedor danés ofrece precios extraordinarios, que comprenden gastos de envío y de internamiento en el país. El ferretero, acudiendo a sus clásicos conocimientos de Derecho, pues años atrás fue un abogado contractualista, está seguro de que, al existir una oferta en la cual se ha identificado plenamente al destinatario (él mismo), el bien objeto de la oferta y el precio, una vez aceptada la oferta, la relación obligacional se habrá consolidado y el proveedor estará obligado a cumplir los términos de su oferta. Sin

embargo, aunque el ferretero envía su giro bancario a las oficinas del proveedor, nunca llegan los productos por los que pagó. Luego descubre que la página web que encontró era una página de fachada y que el proveedor nunca existió.

Como tercer y último escenario imaginemos a dos empresas conocidas mundialmente en la industria de los medicamentos. La empresa A y la empresa B llevan meses negociando una posible fusión, en la que la empresa A absorberá a la empresa B. Uno de los puntos más relevantes de la negociación, si no el principal, es la valorización de unos activos intangibles que se transferirán de una empresa a otra con motivo de la fusión. Esta valorización repercutirá indudablemente en el porcentaje de participación de la empresa absorbida en la empresa absorbente. Así, la empresa A, la absorbente, decide realizar una última oferta de valorización de los activos intangibles, que es aceptada por los ejecutivos de la empresa B, que para comunicar su aceptación con rapidez emplean un medio electrónico. Sin embargo, otra empresa, la C, interesada en absorber la empresa B, y conociendo las negociaciones entre esta y la empresa A, contrata a un experto en informática para que mantenga intervenidos todos los mensajes con destino a la empresa B. De este modo, intercepta el último mensaje remitido por la empresa A, que contenía la última oferta de valorización de los activos intangibles. Modifica su contenido y rechaza la última oferta de valorización definitiva de los activos. Al tener conocimiento del rechazo de la oferta, la empresa A decide terminar las negociaciones con la empresa B. Luego, la empresa C realiza la oferta original de la empresa A y adquiere la empresa B. De este modo, se lleva a cabo una fusión en la que la empresa A debió haber sido la absorbente.

2.8.3. Determinación de los problemas

■ **La identificación de las partes en una operación de comercio**

En el primer escenario y en el segundo es evidente el problema referido a la identificación de las partes. En el caso del niño que ordena las pizzas, el establecimiento que las vende no tendrá cómo saber que el cliente en realidad no es quien dice ser, ya que no ha

existido ningún tipo de contacto físico. En el caso del ferretero, este tampoco tiene la posibilidad de verificar la existencia física de la empresa danesa ofertante, menos aún teniendo en cuenta que ambas partes se encuentran en países diferentes. Este problema surge porque no existe inmediatez física entre las partes que intervienen en una operación de comercio electrónico.

- **La integridad de los mensajes enviados por la red para realizar operaciones de comercio electrónico**

Como hemos señalado, Internet es un medio de comunicación e información que funciona mediante una red abierta, a la cual tiene acceso cualquier persona que cuente con la tecnología adecuada. Al ser una red abierta, cualquier persona con la tecnología adecuada puede entrar en ella e interceptar los mensajes transmitidos por ese medio.

Este problema es graficado en el tercer escenario, en el que, debido a la modificación de un mensaje electrónico, toda una operación de fusión se vio frustrada.

- **La no-repudiación de los mensajes electrónicos**

Se refiere al caso en el cual una persona desconoce el contenido de un mensaje electrónico transmitido por Internet y está vinculado al problema de la identificación de las partes. Para graficarlo emplearemos el segundo escenario, con ciertas modificaciones. Pongámonos en el supuesto de que el ferretero obtiene una oferta de venta del proveedor danés a un precio conveniente y que incluye los gastos de transporte. No obstante, una vez efectuada la transferencia de dinero, el proveedor desconoce los términos de su oferta, y afirma que el precio pagado no incluía los gastos de transporte. Aquí estamos ante la repudiación de una parte del contenido del mensaje electrónico de oferta del proveedor. La repudiación de un mensaje electrónico, como vemos, puede ser parcial o total.

- **La confidencialidad de la información transmitida**

Este problema está vinculado de cierta manera al problema de la integridad de los mensajes, pues en este caso se interceptan los mensajes con el simple propósito de conocer su contenido.

Como vemos, el problema no se limita a la modificación de mensajes. También puede surgir por su simple interceptación. El perjuicio, por lo tanto, se puede ocasionar también con el solo conocimiento de información confidencial. Nos sirve de ilustración el escenario tres, en el cual la empresa C, al tener conocimiento de la oferta inicial de la empresa A, pudo mejorar sus condiciones para desplazarla y así frustrar la operación inicial de fusión.

- **Determinación de la ley aplicable**

Por tratarse de una actividad comercial mundial, las leyes aplicables a una operación de comercio electrónico pueden ser distintas. Por ejemplo, en la publicidad de un producto determinado, la empresa que oferte el producto puede tener su sede principal en el Perú y tener alojada su página web en los Estados Unidos. Además, la publicidad efectuada mediante la página se conocerá en todo el mundo. Un acto de competencia desleal en el Perú puede no serlo en Estados Unidos o en Afganistán, o viceversa. ¿Qué ley se aplicará en el caso de que un proveedor de servicios en Roma considere, al amparo de su normativa, que la publicidad de la empresa peruana es un acto de competencia desleal? ¿La ley del lugar donde se conoce la publicidad, la del lugar donde tiene su sede la empresa o la del lugar en el cual se encuentra alojada su página web? El problema es bastante complejo, y cualquier opción que se tome traerá consecuencias ventajosas y adversas.

Otro ejemplo del conflicto de la ley aplicable se da en el escenario dos. Supongamos que se ha concretado la oferta del proveedor danés, pero que parte de los bienes comprados han llegado al Perú con defectos. En este caso, sería necesario determinar bajo qué ley serán determinados los supuestos de transferencia de la propiedad, el de responsabilidad contractual y extracontractual de ser el caso, las obligaciones del vendedor y los derechos del comprador, para

determinar las responsabilidades. Será aplicable la ley del lugar donde se encuentra alojada la página web del proveedor, la ley del lugar donde tiene su sede principal o la ley del domicilio del ferretero, en el caso de que en el contrato celebrado se haya omitido una mención expresa con respecto a la ley aplicable.

- **Determinación de la jurisdicción competente**

La determinación de la competencia está íntimamente ligada al problema de la determinación de la ley aplicable. Por este hecho, nuestros comentarios respecto de este problema se orientan en el mismo sentido que en el problema de la ley aplicable.

- **Determinación del mérito probatorio de los documentos electrónicos**

En el caso de que no se ejecuten las obligaciones contraídas por medios electrónicos, se debe determinar cuál es el documento en el que basará el acreedor su acción para lograr el cumplimiento de las obligaciones una vez determinadas la ley y la jurisdicción correspondientes. En el comercio electrónico, a diferencia de lo que sucede en el comercio tradicional, no existen los documentos en papel. Se habla de documentos electrónicos, que no pueden ser objeto de una materialización.

¿Dónde estará la prueba de las obligaciones contraídas? ¿Estará contenida en el disco duro en el que se encuentra grabada la oferta correspondiente? ¿En la impresión de la comunicación? ¿En el ordenador? ¿Será posible grabar el mensaje en un disquete y adjuntarlo como medio de prueba?

La determinación del mérito probatorio de los documentos electrónicos es muy importante. En efecto, mientras no se tenga certeza del mérito probatorio de los documentos electrónicos, será imposible conminar al pago a quienes incumplan las obligaciones contraídas por estos medios. Por lo tanto, los acreedores en las operaciones electrónicas estarán desprotegidos, y eso desalentará, en consecuencia, la celebración de contratos por este medio.

■ **Determinación del domicilio legal de los sujetos participantes**
Por último, se ha cuestionado la concepción jurídica del domicilio físico de las personas. En efecto, como se ha señalado al explicar el problema de la determinación de la ley aplicable, los sujetos que llevan a cabo operaciones de comercio electrónico pueden encontrarse en lugares que no son su domicilio físico.

Se habla, por este motivo, del domicilio virtual, es decir, de la ubicación específica de una persona en la red. El domicilio virtual tiene como base el hecho de que los usuarios de la red requieren de un punto de localización específico para poder interactuar en ella. Este punto puede encontrarse, por ejemplo, en el lugar donde se encuentra alojada la página web.

El escenario dos nos muestra con mayor claridad este problema. Supongamos que el proveedor danés ha estado en un crucero de 15 días de duración cuando se han llevado a cabo las fases de ubicación de las partes y de contratación electrónica. En este caso, ¿cuál sería la ley aplicable? Podría ser la del lugar donde se encuentra la sede principal de la empresa, la del lugar donde está alojada la página web del proveedor o la de lugar donde estaba el crucero en el momento de la contratación electrónica.

A nuestro parecer, la ley aplicable para el ofertante de bienes o servicios debe ser la del lugar donde se encuentra alojada la página web del ofertante, es decir, donde se encuentra el servidor que aloja la página, pues se trata de un punto de referencia objetivo y permanente. En el caso de la persona que demanda un bien o servicio, es decir, un *consumer,* la ley aplicable puede ser la del lugar donde tiene su domicilio el proveedor de servicios de Internet.

3. CONCLUSIONES DEL CAPÍTULO

1. Internet es el soporte tecnológico que sirve de plataforma de funcionamiento al comercio electrónico. Inicialmente fue concebido como un sistema de comunicaciones para el Ejército americano, para luego convertirse en un sistema de comunicaciones entre entidades educativas, como universidades y centros de estudios

técnicos. Paulatinamente, la concepción de Internet como un medio de comunicaciones ha cambiado para convertirse en un medio universal de comercio.

2. En sus inicios, el acceso a Internet fue restringido, pues como hemos señalado se concibió como instrumento militar de comunicaciones. En la actualidad, el acceso a Internet se ha masificado y está al alcance de cualquier persona.

3. La masificación del empleo de Internet ha traído consigo la aparición de nuevas instituciones jurídicas y problemas jurídicos, como el empleo de los nombres de dominio y las infracciones de marcas registradas, la infracción de derechos de propiedad intelectual o industrial, la competencia desleal, fraudes cometidos en la red, conflictos de jurisdicción y los problemas derivados del comercio electrónico.

4. El comercio electrónico es la aplicación económica por excelencia del Internet. Lo definimos como el conjunto de relaciones comerciales que se entablan por cualquier tipo de personas mediante soportes electrónicos.

5. Se trata de un medio de comercio con una importante trascendencia económica y es virtual, ya que no requiere de la presencia física de los sujetos o de infraestructura. Es, al mismo tiempo, un medio de comercio de vocación universal, de bajos costos, rápido y vinculado íntimamente con la tecnología de punta.

6. Los elementos del comercio electrónico son los sujetos (*consumer, business* y *government*), los actos de comercio celebrados por los sujetos y la infraestructura de comercio electrónico.

7. Los niveles de comercio electrónico están determinados por los sujetos entre los cuales se entablan las relaciones de comercio. De este modo, existen cuatro niveles: *business to business* (B2B), *business to consumer* (B2C), *consumer to consumer* (C2C) y *business to government* (B2G).

8. Las fases en una transacción de comercio electrónico son las mismas que en las de una operación de comercio tradicional o, en todo caso, muy similares. La diferencia radica en los medios con lo cuales los sujetos participantes se valen para interactuar y tener

relaciones comerciales. Las fases son las siguientes: localización o identificación de las partes (fase de preventa), contratación electrónica y ejecución, y conclusión de los contratos.

9. El comercio electrónico, dadas las características señaladas, es un instrumento de comercio, que puede ser empleado de manera adecuada o inadecuada. Al margen de este hecho, como cualquier otra herramienta, no es perfecto. Presenta una serie de dificultades, que a continuación resumimos.

Dificultades en el comercio electrónico

1. Dificultades financieras o económicas

— Tecnología costosa

Como hemos señalado, la puerta de acceso al comercio electrónico es Internet y, consecuentemente, es la tecnología necesaria para su empleo. Si bien es cierto que el empleo de Internet se ha masificado, los costos para acceder a esta tecnología siguen siendo muy altos, sobre todo en países en vías de desarrollo, como el Perú. Esto sin contar con que el acceso a la tecnología de seguridad para el *e-commerce* es aún más costoso.

Sin embargo, se está superando este obstáculo con la existencia de las cabinas de Internet, que han proliferado en los últimos dos años. En ellas, el costo de acceso a Internet se diluye entre los diferentes usuarios.

— Preparación insuficiente

La falta de una formación adecuada en la tecnología de Internet y sus múltiples aplicaciones, como el *e-commerce*, ha restringido el empleo del Internet al uso del correo electrónico y del chat. Este hecho limita el potencial uso de Internet para el comercio electrónico. Además, la falta de capacitación en esta tecnología ocasiona que se cometan errores en la ejecución de una operación de comercio.

— Infraestructura tecnológica en constante evolución

Implica una constante capacitación y actualización en tecnología, con el correspondiente gasto.

— Los obstáculos que representan las políticas aduaneras de los Estados en los que están domiciliados los sujetos, así como los problemas de doble tributación. ▶

2. Dificultades jurídicas

— La identificación de las partes en una operación de comercio. Al no ser posible el contacto y la identificación física de las partes, se plantea el problema de buscar medios alternativos para lograrlo.

— La integridad de los mensajes enviados por la red. Al ser relativamente sencillo interceptar los mensajes enviados por la red, existe la necesidad de encontrar un método para evitar la interceptación y alteración de los mensajes.

— La no-repudiación de los mensajes electrónicos. Al existir un obstáculo para la identificación de las partes y, por ende, de la autoría de los mensajes, el rechazo de los mensajes, al negar su autoría, es un riesgo latente.

— La confidencialidad de la información transmitida por los sujetos participantes. Este problema es la otra cara de la moneda del problema de la integridad de los mensajes. Así como es posible alterar un mensaje transmitido por la red, es posible tener acceso no autorizado a su contenido.

— Determinación de la ley aplicable. Al ser posible que las partes contratantes se encuentren en lugares distintos y completamente apartados, surge el problema de la determinación de la ley aplicable en una operación de *e-commerce*.

— Determinación de la jurisdicción competente. Se trata de la otra cara de la moneda del problema de la ley aplicable.

— Determinación del mérito probatorio de los documentos electrónicos. Una de las consecuencias del empleo del comercio electrónico es la sustitución de los documentos en papel por los documentos electrónicos, que aún no son plenamente reconocidos como sustitutos de los papeles.

— Determinación del domicilio legal de los sujetos participantes. Las operaciones de comercio electrónico pueden llevarse a cabo en cualquier lugar del mundo donde exista una computadora conectada a Internet. Por este motivo, determinar el domicilio de una persona se convierte en una tarea complicada.

10. Frente a algunos de los problemas jurídicos señalados se han ideado ciertos medios tecnológicos que son instrumentos de

seguridad jurídica para las transacciones de comercio electrónico. Estos medios serán estudiados en el siguiente capítulo.

11. A cualquier medio de seguridad que pretenda resolver determinado problema, sea o no jurídico, no le será suficiente saltar los obstáculos que el empleo de Internet presenta. Será necesario también un cambio en las costumbres de los usuarios de Internet. Como afirma Mariano Maltese,

> Los cambios de costumbres de toda la humanidad llevan largos períodos de adaptación en donde la adopción de un medio de vida tiene que ser comprobadamente aventajado al desechado. Nadie deja un estado de conciencia si no es que está convencido de la virtud superior que significa la nueva experiencia.[24]

Nosotros agregamos que nos encontramos recién en el inicio de este cambio entre estados de conciencia.

---

[24] MALTESE, Mariano. «El pago electrónico en la Argentina – Diversos medios de pago relacionados con el comercio electrónico». En <http://vlex.com/redi/No._39_-Octubre_del_2001/10>.

CAPÍTULO II
Medios de seguridad jurídica en el comercio electrónico

1. Introducción

Como hemos indicado en el capítulo anterior, para que pueda desarrollarse el comercio electrónico a plenitud será necesario contar con las herramientas jurídicas que les garanticen a los sujetos que intervienen en esta actividad que las transacciones que realicen tendrán plena validez. Además, deberán estar seguros de que podrán emplear los mecanismos legales que les permitan exigir los derechos que adquieran en virtud de estas transacciones comerciales. De ahí se deriva la importancia de contar con herramientas de seguridad jurídica especialmente diseñadas para el *e-commerce*.

En este sentido opina Martínez Nadal, haciendo referencia a determinados medios de seguridad:

> En pleno desarrollo de la sociedad de la información, la aplicación de las nuevas tecnologías para el desarrollo de verdaderas transacciones comerciales, la firma electrónica, junto con los certificados y entidades de certificación, se ofrecen, desde el punto técnico, como elementos para conseguir un comercio electrónico seguro a gran escala, en cuanto permite solucionar los problemas de autenticidad, integridad, no

rechazo en origen, e, incluso, en algunos casos, confidencialidad, inherentes a las comunicaciones electrónicas.[1]

De los problemas jurídicos derivados del comercio electrónico, para los fines del estudio de los sistemas de seguridad jurídica en este trabajo solo profundizaremos en los siguientes: la identificación de las partes, la integridad de los mensajes, la confidencialidad de los mensajes, la no-repudiación de los mensajes, el efecto cancelatorio de los medios de pago electrónicos y la eficacia probatoria de los documentos electrónicos.

2. FIRMA DIGITAL

2.1. Introducción

2.1.1. Funciones de la firma tradicional[2]

Con la aparición de nuevas tecnologías para el desarrollo de las comunicaciones, como Internet, y para el desenvolvimiento de sus actividades comerciales, como es el caso del *e-commerce*, los medios y métodos tecnológicos con los cuales se contaba han cambiado. El papel, soporte físico en el cual se dejaba constancia de diversos actos o declaraciones de toda índole, es paulatinamente sustituido por el documento electrónico. De la misma manera, la firma manuscrita (empleada para dar reconocimiento de los actos o declaraciones contenidos en papel y a la vez para dejar constancia de la identidad de una persona) se está reemplazando por la firma electrónica. Por ello, consideramos necesario realizar una breve explicación de las funciones de la firma manuscrita, para luego compararlas con las de la firma digital y, de este modo, comprender su estructura y funcionamiento.

---

[1] MARTÍNEZ NADAL, Apolonia. *La ley de firma electrónica*. Primera edición. Madrid: Civitas Ediciones, p. 17.

[2] CUERVO, José. «La firma digital y entidades de certificación». En <http://www.informatica-juridica.com/trabajos.asp>.

La firma es definida en la doctrina como el signo personal distintivo que permite informar acerca de la identidad del autor de un documento y manifestar su aprobación del contenido del acto.

La Real Academia Española define la firma como «nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice».

En el *Vocabulario Jurídico* de Coutoure se define como «Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad, y obligarse en lo que en ellos se dice».

2.1.2. Características

De las anteriores definiciones de la firma se desprenden las siguientes características:

Identificativa: sirve para identificar al autor del documento.

Declarativa: significa que el autor de la firma asume el contenido del documento. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.

Probatoria: permite verificar si el autor de la firma es efectivamente quien ha sido identificado como tal en el acto de la propia firma.

2.1.3. Elementos

Hemos de distinguir entre elementos formales y elementos funcionales.

- **Elementos formales:** son los elementos materiales de la firma, que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la firma. Son dos:

La firma como signo personal. La firma se presenta como un signo distintivo y personal, ya que debe ser de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

El *animus signandi*. Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido de un documento y no debe ser confundida con la voluntad de contratar, como señala el profesor Larrieu.

- **Elementos funcionales:** tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función.

Identificación. La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. La identidad de la persona nos determina su personalidad para la atribución de derechos y obligaciones. La firma manuscrita expresa la identidad, la aceptación y la autoría del firmante. No es un método de autenticación totalmente fiable. Aun cuando se reconoce la firma, el contenido del documento puede haber sido modificado en cuanto a su contenido, es decir, falsificado. Y en el caso de que no exista la firma autógrafa, al parecer no hay otro modo de autenticación. En caso de duda o negación de la firma, se puede recurrir a una pericia grafotécnica para determinar la autenticidad.

Autenticación. El autor del acto expresa su consentimiento y hace propio el mensaje. Este reconocimiento puede darse en una operación pasiva, que no requiere del consentimiento ni del conocimiento siquiera del sujeto identificado, o en un proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere a él.

2.1.4. Aspectos legales

La firma acredita la autoría del documento suscrito. Normalmente se encuentra al pie del documento y representa la formalización del consentimiento y la aceptación de lo expuesto. Es, por lo tanto, origen de derechos y obligaciones. Por esta razón, en lo posible, una persona debería procurar no variar su firma, pues las funciones de identificación y de autenticación quedarían sin efecto.

La firma, como declaración de voluntad, será válida siempre que no sea falsificada o no se haya obtenido mediante engaño, coacción o cualquier otro proceder ilícito.

2.1.5. Firma electrónica y firma digital

Consideramos oportuno hacer una distinción entre la firma electrónica y la digital. En efecto, no necesariamente son lo mismo, y es común confundir una con la otra.

Citamos el concepto de firma electrónica de Martínez Nadal:

> [...] una firma electrónica será simplemente cualquier método basado en medios electrónicos utilizado o adaptado por una parte con la intención de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita [...][3]

Zárate, por su parte, considera que

> [...] la «firma electrónica» es cualquier símbolo que utilicemos como identificador de una persona en un determinado documento que para su transmisión utilice medios electrónicos, lo cual se asimila a la firma tradicional. El nombre de una persona escrito al final de un documento o un símbolo que le identifique sería una firma electrónica.[4]

La firma electrónica, según estas dos definiciones, es un término muy genérico, en el cual se diluyen las funciones de identificación y de autenticación. Por esta razón, para dotar el concepto de firma electrónica con las funciones mencionadas, debe estar complementado con la indicación de que se debe garantizar que ha sido creada por medios que estén bajo exclusivo control de una persona determinada, de manera que solo esta se encuentre vinculada a su firma. De incumplir con estos requisitos de exclusividad en el uso y de certeza en la identificación, no existirá una firma electrónica como un medio de seguridad jurídico. Sin embargo, la inseguridad de la firma electrónica es evidente, ya que su falsificación es tremendamente sencilla. Su invalidez como método de autenticación de documentos resulta, por lo tanto, obvia.

---

[3] MARTÍNEZ NADAL. Ob. cit., p. 38.

[4] ZÁRATE, Marta: «Caos digital: ¿firma electrónica o firma digital?». En <http://www.derecho.com>.

La firma digital es una especie de firma electrónica. Al igual que la electrónica, es un método basado en medios electrónicos para la identificación y vinculación de una persona. Su rasgo distintivo es el método que se emplea para su creación: la criptografía asimétrica. Esta característica adicional es lo que dota a la firma digital de los atributos de identificación y autenticación. En conclusión, entre estos tipos de firma hay una relación de género (firma electrónica) a especie (firma digital).

2.2. Definición de firma digital

Según Cuervo,

> Las firmas electrónicas o digitales consisten básicamente en la aplicación de algoritmos de encriptación a los datos; de esta forma, sólo serán reconocibles por el destinatario, el cual además podrá comprobar la identidad del remitente, la integridad del documento, la autoría y autentificación, preservando al mismo tiempo la confidencialidad.[5]

Para Ramos Suárez,

> La firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (autenticación) y que no ha existido ninguna manipulación posterior de los datos (integridad) [...] consiste en la utilización de un método de encriptación llamado asimétrico o de clave pública [...][6]

Ambos autores coinciden en que la firma digital es el resultado del proceso de aplicación de un método de encriptación, llamado asimétrico, o de clave pública, que tiene por objeto comprobar la identidad del remitente de un mensaje, la integridad del mensaje, la autoría y, por último, la autentificación. Como se puede apreciar, se diferencia de la firma electrónica en que contiene un elemento

---

[5] CUERVO. Ob. cit.

[6] RAMOS SUÁREZ, Fernando. «La firma digital: aspectos técnicos y legales». En <http://www.marketingycomercio.com/numero14/00abr_firmadigital.htm>.

adicional: el proceso al que se somete para su creación, es decir, la criptografía asimétrica.

La firma digital, como afirma Cuervo,

> Tiene los mismos cometidos que la firma manuscrita, pero expresa, además de la identidad y la autoría, la autentificación, la integridad, la fecha, la hora y la recepción, a través de métodos criptográficos asimétricos de clave pública (RSA, GAMAL, PGP, DSA, LUC, etc.), técnicas de sellamiento electrónico y funciones Hash, lo que hace que la firma esté en función del documento que se suscribe (no es constante), pero que la hace absolutamente inimitable como no se tenga la clave privada con la que está encriptada, verdadera atribución de la identidad y autoría.[7]

Como vemos, la firma digital tiene las mismas funciones que la manuscrita. Es un signo personal, identifica a su titular, autentica el contenido del acto que se firma y, además, tiene algunas funciones adicionales, que han sido mencionadas. Podemos concluir que la firma digital es simplemente una respuesta tecnológica frente a nuevas formas de realizar operaciones comerciales.

Como afirma Cuervo, la criptografía asimétrica se sustenta en el mensaje que se quiere cifrar. Se trata de un método seguro, ya que la encriptación que se realiza no es estándar, sino que dependerá de las características de cada mensaje cifrado.

Más adelante desarrollaremos ciertos conceptos necesarios para entender el funcionamiento de la firma digital: la criptografía y la función Hash.

2.3. Características de la firma digital

A partir de las definiciones podemos señalar las características de la firma digital.

- Debe permitir la identificación del signatario. Para lograrlo debe estar asociada únicamente a él. Entramos en el concepto

[7] CUERVO. Ob. cit.

de autoría electrónica, es decir, la forma de determinar que una persona es quien dice ser en la esfera de las relaciones entabladas por medios electrónicos.

Esta característica es tomada en cuenta en las *ABA Guidelines*[8] en los siguientes términos: «Una firma debe indicar quién firmó un documento, mensaje o récord, y debe ser difícil para otra persona producirla sin autorización».

- No puede ser generada más que por el emisor del documento. Debe ser infalsificable e inimitable, es decir, solamente el firmante está en capacidad de controlar la generación de la firma digital que lo identifica.
- Las informaciones que se generen a partir de la signatura electrónica deben ser suficientes para validarla pero insuficientes para falsificarla.
- Debe permitir detectar la alteración de los mensajes.
- Debe contener los elementos necesarios para probar la participación del signatario en la emisión del mensaje que ha sido firmado digitalmente. En otras palabras, debe facilitar la no-repudiación de los mensajes.
- Por último, de acuerdo con las *ABA Guidelines*, la firma digital autentica documentos. Una vez identificado lo firmado, es imposible falsificar o alterar el documento firmado o la firma sin que este acto sea detectado.

---

[8] La American Bar Association es la asociación más grande de profesionales voluntarios en el mundo, con más de 400 mil miembros. La ABA proporciona acreditación de facultades de derecho, educación legal continua, información sobre derecho, programas de asistencia a jueces y abogados en su trabajo, e iniciativas para mejorar el sistema legal para el público. Para mayor información véase <http://www.abanet.org/home.html>. Esta entidad ha publicado una *Guía de firmas digitales (Digital Signature GUIDELINES)*. Dicho documento, conocido como las *ABA Guidelines*, menciona determinados estándares que deben seguir las firmas digitales para cumplir con su función de brindar seguridad jurídica.

2.4. Naturaleza jurídica de la firma digital

Una vez determinados el concepto y las características de la firma digital, podemos inferir que su naturaleza jurídica es la de un medio de identificación de la persona que emplea la firma, un medio que vincula a la persona con los actos que declara en el mensaje firmado y un medio de certificación de los mensajes que se envían.

En resumen, es un medio de prueba de la manifestación de voluntad, de la autoría de un mensaje y de su integridad. Al ser un medio de prueba, como hemos mencionado, se convierte en un medio de seguridad jurídico, ya que el Derecho le otorga plena validez. Con esto se evitarán situaciones de inseguridad y de falta de certeza en las operaciones de comercio electrónico.

En conclusión, la naturaleza jurídica de la firma digital es la de un medio de seguridad, cuya función probatoria permite la identificación de una persona y de la autoría de un mensaje, además de asegurar la integridad del mensaje.

2.5. Elementos de la firma digital

Creemos conveniente precisar cuáles son los elementos que permiten la creación de una firma digital y su posterior verificación. Para este cometido nos valdremos del real decreto ley 14/1999 (en adelante, el real decreto ley) emitido por el Estado español.

2.5.1. Datos de creación y verificación de la firma digital

- Definición

El real decreto ley establece como definición de datos de creación los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica. Los datos de verificación son, en cambio, los datos como códigos o claves criptográficas públicas que se utilizan para verificar la firma electrónica.

Los datos de creación y de verificación de firma están vinculados a la clave privada y a la clave pública que se emplean en el sistema de criptografía asimétrica que desarrollaremos más adelante. Como

afirma Martínez Nadal, «[e]n definitiva, los datos de creación y verificación de forma nos sitúan ante el par de claves asociadas en que, como hemos visto, se basan los criptosistemas de clave pública».[9]

- **Calidad en la generación de los datos**

Para que la firma digital cumpla con su función de medio de seguridad, será necesario que los datos de creación y de verificación de la firma sean seguros y de calidad.

Entramos así en la cuestión de la calidad en la generación de los datos de la firma digital, la cual debe reunir ciertas condiciones para que sea considerada de calidad.

El par de claves debe ser seguro.

La seguridad en el par de claves está determinada por su irreversibilidad, es decir, para que el par de claves sea considerado seguro, no deberá ser posible obtener la clave privada utilizando la clave pública.

Esta característica dependerá de la longitud de la clave y de los avances de la técnica. Como afirma Martínez Nadal:

> Los algoritmos más comunes para la codificación mediante el empleo de claves públicas y privadas se basan en una característica importante de los grandes números primos: una vez que se multiplican entre sí para producir un nuevo número es virtualmente imposible determinar cuáles fueron los números primos que crearon ese nuevo número más grande [...][10]

De esta cita se desprende que la solución para la irreversibilidad se encuentra en parte en las matemáticas, precisamente en los algoritmos. La irreversibilidad del proceso, que es la esperanza de que será imposible derivar la clave privada secreta de un usuario a partir de su clave pública, se llama *no viabilidad computacional*. Se trata de un concepto relativo basado en el valor de los datos protegidos.

---

[9] MARTÍNEZ NADAL. Ob. cit., p. 49.

[10] Ibíd., p. 51.

La irreversibilidad estará determinada por el valor de los datos protegidos, la capacidad computacional general requerida para protegerlos, el tiempo necesario para protegerlos, el costo y el tiempo necesarios para atacar esos datos. En función de estos factores se habla de una seguridad incondicional o teórica (es decir, un sistema seguro frente a un atacante con tiempo y recursos computacionales ilimitados) y de una seguridad computacional o práctica (un sistema seguro frente a un atacante con tiempo y recursos limitados).

El par de claves debe ser único.

La unicidad de las claves implica que no deben existir dos o más juegos de claves iguales. De no ser así, la función de identidad no podría existir. Por este motivo, los procedimientos de generación de claves deben introducir los elementos de aleatoriedad necesarios para evitar que dos personas que estén utilizando el mismo programa de generación obtengan una clave igual. Esta posibilidad podría darse en los casos de homonimia, en los cuales algunos de los datos de creación de firma podrían ser iguales.

Al margen de la unicidad del par de claves, surge la pregunta de si una misma persona puede tener más de una firma digital. Si una de las funciones de este medio de seguridad es la identificación de una persona, ¿cómo podría existir más de una firma digital para una persona? Si fuera el caso, ¿cuál de las dos firmas la identificaría? ¿todas sus firmas cumplirían la misma función?

Creemos que a diferencia de lo que ocurre con la firma manuscrita, en la que una persona solo puede tener una firma determinada, en el caso de la firma digital la tecnología permite que una persona pueda tener varias firmas, cada una para un fin específico. Para esto, en nuestra opinión sería necesaria la intervención de la entidad de certificación para que, al asociar la firma con su titular, describa cuál es el uso específico de cada una de las firmas. De esta manera, los terceros que se vinculen con una persona que tenga más de una firma digital podrán saber cuál es el uso específico que le da el titular a una de sus firmas.

En todo caso, si existiesen reparos respecto de esta posibilidad, podrían establecerse determinados supuestos únicamente en los cuales la entidad de certificación, a su propia discreción, podría optar por certificar dos o más firmas digitales adicionales.

El procedimiento de generación debe ser adecuado.

Un procedimiento de generación adecuado impedirá que personas no autorizadas obtengan la clave privada reproduciendo el procedimiento de generación de claves. La calidad de las claves de criptografía asimétrica puede variar en función del sistema de creación del par de claves.

Existen dos tipos de mecanismos de generación de claves. En uno es el propio titular de las claves quien las genera, con la ventaja de que la destrucción de la clave privada será efectivamente llevada a cabo para que solo el titular de la firma conozca la clave. En el otro mecanismo es una entidad de certificación la que genera el par de claves. La ventaja de este sistema es que genera claves de mayor calidad y con mayores garantías, ya que se empleará una tecnología que estará al alcance de más personas.

Como podemos apreciar, ambos sistemas de generación de claves tienen ventajas y desventajas. En conclusión, podemos afirmar que, al margen del sistema utilizado, lo importante es que las claves sean únicas y a prueba de manipulaciones. Además, es esencial que la clave privada esté bajo el exclusivo control del titular de la firma digital.

2.5.2. *Dispositivos de creación y verificación de firma digital*

- **Definición**

Los dispositivos de creación y de verificación de firma, de acuerdo con lo establecido por el decreto ley, son «[...] un programa o un aparato informático que sirve para aplicar los datos de creación de firma, y un programa o aparato informático que sirve para aplicar los datos de verificación de firma», respectivamente.

Como afirma Martínez Nadal,

> [...] se trataría respectivamente de aquellos elementos informáticos que permiten la aplicación de la clave privada sobre un mensaje electrónico por parte de su autor y remitente para la creación de una firma electrónica; y la aplicación de la clave pública por parte del destinatario para la verificación de ese mensaje firmado electrónicamente.[11]

Como señalan estas dos definiciones, los dispositivos de generación y verificación de firma constituyen la dimensión dinámica de los elementos de la firma digital. Los datos de generación y de verificación de firmas son un elemento estático. Son la base de datos de la firma, mientras que los dispositivos de generación y verificación son el uso de los datos.

Los dispositivos de generación y verificación son tan importantes, o más, que los datos de generación y de verificación, ya que de ellos depende que la exactitud de los datos proporcionados sea correctamente empleada. Por este motivo, los dispositivos deben reunir ciertos requisitos que garanticen su correcto funcionamiento.

- **Dispositivo seguro de creación de firma**

Un dispositivo seguro de creación de firma será el programa o aparato informático que aplica el dato de creación de firma (la clave privada) sobre un mensaje electrónico, cumpliendo una serie de requisitos.

La implicancia de calificar a un dispositivo de creación de firma electrónica como seguro tiene como consecuencia jurídica que se dotará a la firma de plena eficacia jurídica, equiparando sus efectos a los de la firma manuscrita.

Del mismo modo, una firma electrónica generada mediante un dispositivo seguro de creación de firma tendrá plena eficacia probatoria en materia procesal. Este hecho demuestra la gran importancia de que se lleve a cabo con rigurosidad la calificación de seguridad de un dispositivo de creación y verificación de firmas.

---

[11] Ibíd., p. 56.

- **Requisitos para la calificación de seguridad**

- Que garantice que los datos utilizados para la generación de firmas puedan producirse una sola vez y que asegure razonablemente su secreto.

  Este requisito va en correspondencia con la unicidad de los datos de creación y verificación de firmas. Como indicamos al iniciar el tema de los dispositivos de generación y verificación, de nada valdría que los datos de creación y verificación de firma fueran únicos si los dispositivos no garantizaran la generación de claves únicas.

- Que exista una seguridad razonable de que los datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología vigente.

  Este requisito está relacionado con la característica de irreversibilidad de las claves en un sistema de criptografía asimétrica.

  Es importante recalcar que los sistemas de creación de firmas solo pueden considerarse seguros dentro de un plazo razonable, ya que la evolución de la tecnología facilita la violación de las claves creadas por sistemas que han estado en circulación por un tiempo. Si tenemos en cuenta la rápida evolución de la tecnología, un dispositivo de creación o de verificación de firma no podrá ser 100% seguro por un período demasiado prolongado. En efecto, a medida que se desarrolle la tecnología será más sencillo violar la seguridad del dispositivo.

- Que los datos de verificación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

  Este requisito es indispensable para determinar fiablemente la autoría de un mensaje. Si el dispositivo no garantiza la imposibilidad del empleo de los datos por terceras personas, no existirá una forma de conocer cuál es el verdadero autor de un mensaje.

  Es conveniente señalar que para el cumplimiento de este requisito será necesaria la participación del titular de la firma digital, quien deberá cautelar que la clave secreta sea de su único y exclusivo conocimiento. Un dispositivo de generación y de

verificación de datos puede ser infalible, pero si el titular de una firma no protege adecuadamente su clave, no será posible asegurar que el titular es efectivamente el autor de un mensaje determinado.

- Que el dispositivo utilizado no altere los datos o el documento que deba firmarse, ni impida que se muestre al signatario antes del proceso de firma.

  Respecto de la primera afirmación, debemos tener en cuenta que las funciones de la firma digital no deben superponerse sino coexistir. De lo contrario, su eficacia sería parcial. No se pude sacrificar la identidad de los mensajes por determinar la autoría. Por esta razón, uno de los requisitos de un dispositivo seguro de creación y verificación es que no modifique los mesajes enviados.

  Del mismo modo, un dispositivo seguro deberá permitir al autor de un mensaje tener acceso al contenido. Si esto no ocurre, la autentificación de la firma será imposible. En efecto, si el autor del mensaje no puede tener conocimiento del contenido del mensaje, será imposible vincularlo jurídicamente a su mensaje.

■ Procedimiento de certificación

Una vez descritas las características que deberían tener los dispositivos de creación y de verificación de firma, el siguiente paso es determinar cómo y quién deberá darle la certificación de seguridad al sistema.

El debate se inicia con la interrogante de quién debe prestar la certificación: el Estado (mediante el organismo correspondiente) o el sector privado. La respuesta a esta pregunta la planteamos en los mismos términos en que responderemos quién debe prestar los servicios de certificación, es decir, deberá ser una entidad de certificación (o tercera parte de confianza) que al mismo tiempo certifique productos de firmas electrónicas, ya sea del sector público o del privado.

La expedición de la certificación se deberá realizar antes de la realización de un informe técnico sobre los dispositivos, que deberá ser emitido por entidades acreditadas de evaluación.

2.6. Funciones de la firma digital

Recurriremos a las *ABA Guidelines* para determinar las funciones de la firma digital.

Evidencia. Una firma identifica a un suscriptor con el documento firmado. Cuando el suscriptor realiza una marca distintiva, el escrito es atribuible al suscriptor.

Con esta función se impide la repudiación de los mensajes enviados, es decir, una vez que una persona suscribe un documento se vincula a él y a los actos que constan en él, de acuerdo con las condiciones acordadas.

Solemnidad. El acto de firmar un documento hace que el suscriptor sea consciente de la formalidad que se requiere para que la firma surta los efectos deseados. De esta manera, una firma digital que reúna los requisitos mencionados cumplirá con las formalidades requeridas para que surta efectos jurídicos.

Aprobación. En determinadas situaciones definidas por la ley o la costumbre, una firma expresa la aprobación del suscriptor, la autorización del escrito o la intención del suscriptor de que el documento tenga efectos legales. Se trata de la función de autentificación, en virtud de la cual el suscriptor de un documento presta su conformidad con el contenido legal de un contrato y acepta vincularse en los términos en él establecidos.

Eficiencia y logística. La firma en un documento escrito imparte con frecuencia un sentido de claridad y de finalidad a una transacción. Además, puede reducir la necesidad de realizar requerimientos que excedan lo establecido en el documento. La idea de la claridad y la finalidad es determinar con exactitud el contenido del documento para determinar los términos en los cuales se obliga su suscriptor.

La firma digital permite que los documentos suscritos sean fácilmente intercambiables al no ser necesario el traslado del documento físico sino, únicamente, el envío del documento electrónico. Este hecho implica mayor facilidad, rapidez y fluidez en el intercambio de documentos.

2.7. El mecanismo de funcionamiento de la firma digital

2.7.1. La criptografía

■ Introducción

Como hemos señalado, la firma digital se distingue de la firma electrónica en que la primera emplea la criptografía asimétrica como método para identificar al autor y el contenido de un mensaje, entre otros fines.

Uno de los problemas jurídicos que se presentan en el *e-commerce* es la facilidad con que los mensajes enviados por Internet pueden ser interceptados y modificados con la tecnología apropiada. En otras palabras, existen riesgos en las comunicaciones entabladas entre quienes intervienen en una transacción de *e-commerce*.

Como afirma Luciano Moreno, «[p]ara establecer una comunicación de datos entre dos entidades (personas, equipos informáticos, etc.) hacen falta al menos tres elementos básicos: el emisor del mensaje (la fuente), el receptor del mensaje (el destino) y un soporte físico por el cual se transfieren los datos (el medio)».[12]

Según la importancia de los mensajes se elegirá el medio apropiado para su transmisión. Por ejemplo, los mensajes que no tengan un contenido privado, confidencial o muy importante podrán ser transmitidos por medios que permitan que personas distintas a los destinatarios tengan acceso a ellos. Es el caso de la publicidad de un bien o de un servicio. Para transmitir, en cambio, un mensaje cuyo contenido sí sea confidencial o importante se requerirá de un medio que garantice que solo tendrá acceso a él el destinatario (por ejemplo, en el caso de la oferta de compra de un bien determinado).

El medio por excelencia para enviar mensajes ocultos es la criptografía. De ella se sirven Internet y el comercio electrónico para asegurar la confidencialidad de los mensajes enviados por la red.

---

[12] MORENO, Luciano. «Criptografía». En <http://www.htmlweb.net/seguridad/cripto/cripto_1.html>.

■ Definición

La criptografía (de *kriptos*, 'ocultar', y *graphos*, 'escritura') es una técnica que consiste en cifrar (ocultar) y descifrar (revelar) mensajes. En otras palabras, transforma un mensaje inteligible (el texto en claro) en otro que solo puedan entender las personas autorizadas (el criptograma o texto cifrado).

La criptografía, como afirma Moreno,

> [...] es una rama de las matemáticas que se complementa con el criptoanálisis, que es la técnica de descifrar textos cifrados sin tener autorización para ello, es decir, realizar una especia de criptografía inversa. Ambas técnicas forman parte de la ciencia llamada criptografía.[13]

Los sistemas criptográficos pueden ser muy simples, como el reemplazo de cada letra del alfabeto por la tercera letra que le sigue. Según este sistema, «Julio César» se escribiría «Mxolr Fhvdu». Pero también pueden ser muy complejos, recurriendo a las matemáticas.

Cuanto más complejo sea el sistema criptográfico empleado será más difícil descifrar el mensaje ocultado. Se recurre a las matemáticas para estructurar sistemas complejos que permitan una mayor seguridad de los mensajes ocultos.

■ Criptografía clásica

El cifrado de textos se ha realizado a lo largo de la historia. Para muestra basta el sistema criptográfico empleado en la época de Julio César al que nos hemos referido. De acuerdo con este sistema, en nuestro alfabeto actual tenemos las siguientes equivalencias:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

De acuerdo con esta tabla de equivalencias, la expresión «comercio electrónico» serían cifradas como «frohuflr hñhfwuplfr'.

---

[13] Ibíd.

En la época en que fue implementado este sistema era muy útil y efectivo. Sin embargo, con el paso del tiempo se volvió obsoleto y vulnerable, por lo que fue necesario recurrir a otros métodos de ocultación.

La sustitución

Consiste en cambiar los caracteres del mensaje original por otros según una regla determinada de posición natural en el alfabeto. Una posible tabla de equivalencias de acuerdo con este sistema de ocultación es la siguiente:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I

Según esta tabla, la expresión «comercio electrónico» cifrada serían «lxunalqx ntnlcavqlx».

No es necesario que el alfabeto equivalente esté ordenado naturalmente. Puede estar en cualquier otro orden. Solo se exige que tenga todos y cada uno de los elementos del alfabeto original.

Este tipo de sustitución se denomina monoalfabético. Existen métodos más eficaces, como los polialfabéticos, en los que varios alfabetos de cifrado se emplean en rotación.

- **La transposición**

Consiste en cambiar los caracteres del mensaje original por otros según una regla determinada de posición en el orden del mensaje. Por ejemplo, si establecemos la siguiente regla de cambio en el orden de las letras en el texto:

la letra	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
pasa a ser la	6	1	4	8	9	2	3	5	7	19	13	16	18	12	10	14	17	15	11

En esta tabla de equivalencias, la primera fila de números representa el orden de las letras de las palabras que se desee cifrar. Los números de la segunda fila representan el nuevo orden que tendrán las letras de las palabras encriptadas.

Desdoblando la tabla tenemos, en primer lugar, el número de orden de las palabras que se van a cifrar:

la letra	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	C	O	M	E	R	C	I	O	E	L	E	C	T	R	O	N	I	C	O

En segundo lugar, tenemos el nuevo orden de las letras de las palabras que se van a cifrar:

pasa a ser la	6	1	4	8	9	2	3	5	7	9	13	16	18	12	10	14	17	15	11
	O	C	I	M	O	C	E	E	R	O	O	R	E	N	C	C	I	T	I

Entonces, de acuerdo al sistema de criptografía por transposición, las palabras «comercio electrónico» se cifrarían como «ocimoce eroorencciti».

2.7.2. Claves

Como señala Moreno, el primer obstáculo al descifrar un mensaje cifrado —sea por sustitución o por transposición— es recordar cuál fue el método empleado para camuflar el mensaje. Una posible solución, como afirma el autor, es indicar el método en un soporte cualquiera (papel, disquete, etc.). Sin embargo, esta posibilidad conlleva el riesgo de que el soporte llegue al alcance de terceras personas que lo utilicen para fines ilícitos.

Una mejor solución sería implementar un mecanismo de sustitución o permutación que esté basado en una sola palabra corta o clave. Emplearemos el ejemplo de Moreno.[14]

Supongamos que queremos cifrar la frase «Hola mundo» basándonos en la palabra «html». Para ello escribimos una tabla o matriz con tantas columnas como letras tenga la palabra elegida y colocamos la palabra en la fila superior. Situamos el mensaje a cifrar en las filas siguientes y si sobran celdas las dejamos vacías.

[14] Ibíd.

H	T	M	L
H	O	L	A
M	U	N	D
O			

El paso siguiente será cambiar el orden de las filas. Por ejemplo, poniendo las letras de la palabra elegida en orden alfabético, con lo que nuestra tabla queda así:

H	L	M	T
H	A	L	O
M	D	N	U
O			

Por último, podemos transformar las filas de la tabla en columnas:

H	H	M	O
L	A	D	
M	L	N	
T	O	U	

Solo nos falta obtener el nuevo mensaje, leyendo las filas obtenidas: «HOLA MUNDO» se convierte en «HHMO LAD MLN T».

Para descifrar el texto cifrado habrá que realizar las operaciones anteriores en sentido inverso.

La ventaja de este sistema es que, si el método de cifrado es complejo, será fácil recordarlo con la clave, que además será más fácil de proteger contra terceras personas.

Esta palabra o serie determinada como base del mecanismo de cifrado se denomina *clave de cifrado*. El número de letras que la forman se llama *longitud de la clave*.

2.7.3. Criptografía moderna

El sistema criptográfico que hemos descrito presenta dos obstáculos principales: la longitud de la clave empleada (de la que dependerá la eficiencia del sistema, como hemos visto) y el tiempo necesario para cifrar y descifrar los mensajes.

Como indica Moreno,[15] estos obstáculos han sido superados por los siguientes factores:

Velocidad de cálculo. La aparición de las computadoras ha contribuido con una potencia de cálculo superior a los métodos anteriores.

El avance de las matemáticas. Las matemáticas permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros.

Necesidades de seguridad. Surgieron muchas actividades nuevas que precisaban la ocultación de datos, con lo que la criptología experimentó un fuerte avance.

Estos factores han contribuido a la aparición de sistemas criptográficos como el simétrico o el asimétrico, que a continuación desarrollaremos.

2.7.4. Clases

Pueden existir infinitos sistemas de cifrado, como hemos mencionado. Para los fines de este trabajo describiremos los dos sistemas más usados en el comercio electrónico, que están basados en la criptografía moderna.

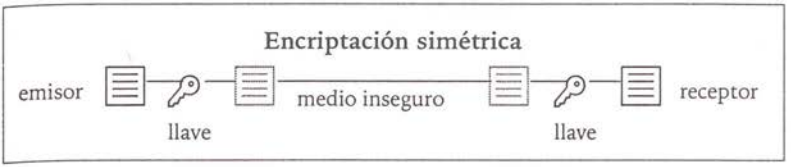
- **Sistema de clave secreta o criptografía simétrica**

Este sistema emplea solo una clave, conocida tanto por el autor de un mensaje como por su destinatario. Debe ser acordada previamente.

---

[15] Ibíd.

Es llamado simétrico porque el autor y el destinatario de un mensaje tienen conocimiento de la clave. La siguiente figura grafica el funcionamiento de este sistema.[16]



Como se puede apreciar en el gráfico, el emisor emplea la misma clave para cifrar el mensaje que la que usa el receptor para descifrarlo.

Para que este sistema sea seguro es necesario que el emisor y el receptor mantengan la clave en secreto. Según Moreno, para que un algoritmo de este tipo sea considerado seguro debe cumplir con los siguientes requisitos básicos:

- Que, una vez conocido el criptograma (mensaje cifrado), no se puedan obtener a partir de él ni la clave ni el texto cifrado.
- Conocidos el texto en claro (u original) y el texto cifrado, debe implicar un costo mayor en tiempo o en dinero descifrar la clave que el valor posible de la información obtenida por terceros. De esta manera, se desalienta económicamente la violación del sistema.

La evidente desventaja de este sistema radica en la falta de seguridad respecto a la autoría de un mensaje, ya que la clave con la cual se cifran los mensajes no estará bajo exclusivo dominio del titular. Por ello, no es posible garantizar que la clave no haya sido empleada de forma ilícita.

Las desventajas de este sistema se pueden resumir de la siguiente manera:

---

[16] Ibíd.

Distribución de claves. La entrega de claves debe realizarse por un medio altamente seguro. El medio más seguro podría ser la entrega de persona a persona, que obstaculiza el flujo de las transacciones.

Validez frente a terceros. Debido a que se emplea la misma clave para cifrar y para descifrar, es imposible determinar quién es el emisor y quién es el destinatario.

Administración de claves. Se requiere una clave diferente para cada persona con quien uno quiera comunicarse. Al respecto, afirma Herrera:

> El precio que se paga es el hecho que para cada par de usuarios que se quiera establecer una comunicación segura se requiere una clave distinta. Si hacemos cuentas, vemos que de este modo un usuario de una red debe almacenar tantas claves como personas con las que desee mantener una comunicación segura.[17]

Sin embargo, la ventaja que presenta frente al sistema asimétrico es que este resulta más costoso, ya que requiere una infraestructura tecnológica.

- **Sistema de clave pública o criptografía asimétrica**

A diferencia del sistema de criptografía simétrica, en el cual existe una sola clave para cifrar y para descifrar mensajes, en el sistema de clave pública existen dos claves: una para cifrar un mensaje (la clave privada) y otra para descifrarlo (la clave pública). La propiedad fundamental de las claves radica en que una descifra lo que la otra ha cifrado. Es imposible descifrar el mensaje cifrado por una clave, sin su correspondiente par.

En este sistema criptográfico entran en juego los datos y los dispositivos de generación y de verificación de la firma digital que, como hemos señalado, son los elementos de esta firma. De esta manera, los datos y dispositivos de generación de firma estarán

---

[17] HERRERA JOANCOMARTÍ, Jordi. «Criptografía de Clave Pública». En <http://www.iec.csic.es/criptonomicon/articulos/expertos44.html>.

vinculados con la clave privada de una persona, mientras que los datos y dispositivos de verificación de firma estarán vinculados con su clave pública.

Nos remitimos a nuestros comentarios en el apartado 2.5 de este capítulo[18] respecto de las características y funciones del par de claves empleadas en este sistema criptográfico. Como afirma Moreno,

> Las claves pública y privada tienen características matemáticas especiales, de tal forma que se generen siempre a la vez, por parejas, estando cada una de ellas ligada intrínsecamente a la otra, de tal forma que las dos llaves públicas son diferentes, entonces sus llaves privadas asociadas también los son, y viceversa [...]. Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy difíciles de realizar en sentido inverso, salvo que se conozca la clave privada, como la potencia y el logaritmo. Ambas claves, pública y privada, están relacionadas matemáticamente, pero esta relación debe ser lo suficientemente compleja como para que resulte muy difícil obtener una a partir de la otra.[19]

En el mismo sentido señala Herrera:

> Estas claves tienen la asombrosa propiedad que cada una de ellas invierte la acción de la otra pero, y aquí está el punto más relevante, a partir de una no se puede obtener la otra.[20]

Como afirman los autores citados, es imprescindible la asociación de las matemáticas con este sistema para garantizar su inviolabilidad.

En este sistema, la única clave que debe ser mantenida en secreto es la privada, pues debe ser ampliamente difundida la clave pública. Este hecho evita el inconveniente de la distribución de claves y de la confidencialidad de los mensajes, pues la clave privada siempre se mantendrá oculta. Evita también el problema de la

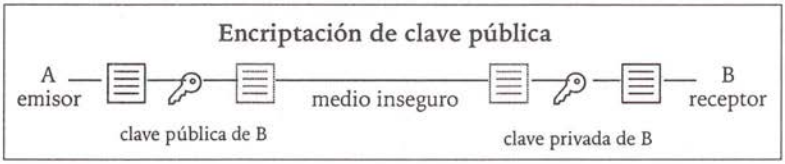
---

[18] Véase la página 81.

[19] MORENO. Ob. cit.

[20] HERRERA JOANCOMARTÍ. Ob. cit.

autoría del mensaje en el sistema simétrico, ya que cada persona tendrá una clave privada de su exclusivo conocimiento y utilización. En otras palabras, es innecesario poner en peligro la clave privada. Nos serviremos del siguiente gráfico para explicar el funcionamiento de este sistema.[21]



Fuente: MORENO, Luciano. «Criptografía». En <http://www.htmlweb.net/seguridad/cripto/cripto_1.html>.

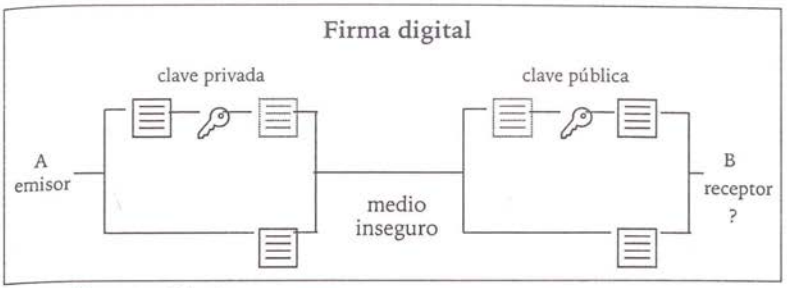
En este gráfico, A desea enviar un mensaje a B empleando el sistema de criptografía asimétrica, para lo cual debe obtener la clave pública de B. Una vez obtenida la clave, cifra el mensaje con ella y lo envía a B. Cuando B recibe el mensaje, lo descifra con su clave privada.

De esta manera, se muestra la interacción de la clave pública y de la privada: lo que una clave cifra, la otra descifra. En el caso descrito en este gráfico, lo que se pretende es garantizar que el mensaje sea transmitido con seguridad (es decir, en forma confidencial e íntegra).

Pero, lo que se puede buscar con el uso de este sistema es garantizar la autoría de un mensaje, posibilidad en la que entra a tallar la firma digital. El gráfico de la página siguiente nos muestra cómo sería el funcionamiento del sistema para este caso.

En este caso, al ser el objetivo garantizar la identidad de A, este cifrará su mensaje con su clave privada y lo transmitirá a B. Una vez que B reciba el mensaje lo descifrará con la clave pública de A. Un mensaje cifrado con la clave privada de una persona solo puede ser descifrado con su clave pública. En el ejemplo citado, el mensaje

[21] MORENO. Ob. cit.



Fuente: MORENO. Ob. cit.

cifrado por A solo podrá ser descifrado con su clave pública. De esta manera, B podrá estar seguro de la identidad de A siempre y cuando pueda descifrar el mensaje enviado por A con su clave pública. Si esto no es posible, se deberá entender que A no es el autor del mensaje enviado.

Para que este sistema sea considerado seguro, debe cumplir con los siguientes requisitos:

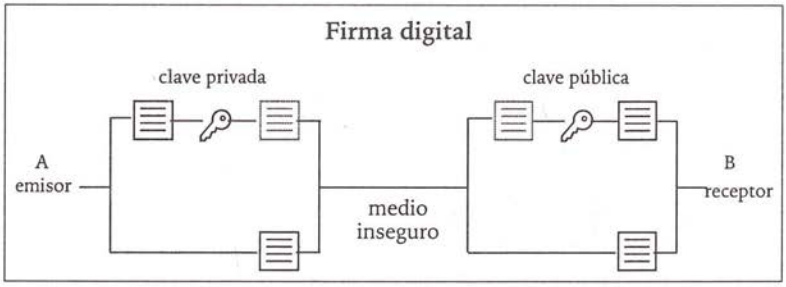
- Conocido el texto cifrado, no debe ser posible encontrar el texto en claro ni la clave privada.
- Conocido el texto cifrado (criptograma) y el texto en claro, descifrar la clave debe resultar más caro en tiempo y dinero que el valor de la información obtenida por terceros.
- Conocida la clave pública y el texto en claro no debe ser posible generar un criptograma correcto cifrado con la clave privada.
- Dado un texto cifrado con una clave privada, solo existe una clave pública capaz de descifrarlo y viceversa.

Como se puede apreciar, el problema de la seguridad quedaría del todo solucionado con los sistemas de clave pública. Sin embargo, es inevitable formularse las siguientes preguntas: ¿cómo sabemos que la clave pública de un usuario pertenece al usuario del que dice ser?, ¿cómo es posible asegurar que usamos la clave pública de quien queremos que reciba nuestro mensaje y no otra clave que alguien ha publicado con una identidad falsa para suplantar a nuestro interlocutor real? Las respuestas a estas interrogantes

están en la participación de las entidades de certificación, de las cuales nos ocuparemos más adelante.

2.8. Función Hash

Nos valdremos de la explicación realizada por Moreno para el estudio de la función Hash. Recordemos el esquema básico de una firma digital:



Fuente: MORENO. Ob. cit.

El proceso de firma digital consta de dos partes bien diferenciadas:

Proceso de firma: en el que el emisor encripta el documento con su clave privada, enviando al destinatario tanto el documento en claro como el cifrado.

Proceso de verificación de la firma: el receptor desencripta el documento cifrado con la clave pública de A y comprueba que coincide con el documento original, hecho que atestigua de forma total que el emisor ha sido efectivamente A.

El método de la firma digital no solo proporciona autenticidad al mensaje enviado por A, sino que también asegura que el mensaje no será repudiado. En efecto, solo el dueño de una clave privada puede cifrar un documento de forma que se pueda descifrar con su clave pública. Esta restricción garantiza que ha sido A y no otro el que ha enviado el documento. Además, asegura la integridad de los

datos, ya que, si en el camino alguien accede al documento y lo modifica, el resumen del documento cambiará también.

La firma digital suele usarse en comunicaciones en las que no existe una confianza inicial total entre los comunicantes. Se usa para autentificar mensajes, para validar compras por Internet, para realizar transferencias de fondos bancarios y para otras transacciones de negocios. Tanta es la fuerza de este sistema que legalmente la firma electrónica es, en la mayoría de los casos, una prueba indubitable de autoría del envío de un documento electrónico, semejante a la firma tradicional de puño y letra.

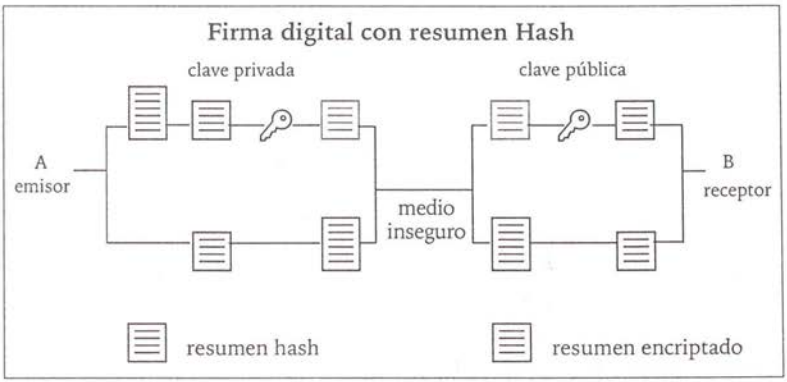
Un alegato que podría esgrimir A para negar la autoría del envío de un documento cifrado con su clave privada sería que ha perdido o le han robado la clave. Pero hay que tener en cuenta que A es el único responsable del buen uso de su clave privada. Por este motivo, está obligado a comunicar inmediatamente a la autoridad correspondiente cualquier circunstancia que ponga en peligro la seguridad de la clave. Este hecho es análogo al que ocurre con las tarjetas de débito o crédito: en último extremo, el dueño de la tarjeta siempre es responsable de su uso indebido si no ha avisado a tiempo a su entidad financiera o a su banco de la pérdida o sustracción.

De acuerdo con lo que afirma Moreno,[22] el proceso de cifrado de un documento entero es una pérdida de tiempo. Esto se debe a que los medios de encriptación de clave pública son lentos, pues precisan un gran proceso de cómputo. Por esta razón, aparecen las funciones Hash. Se trata de funciones matemáticas que realizan un resumen del documento a firmar y cifrar. Comprimen el documento en un único bloque de longitud fija, cuyo contenido es ilegible y no tiene ningún sentido real. Tan es así que por definición las funciones Hash son irreversibles, es decir, a partir de un bloque comprimido no se puede obtener el bloque sin comprimir. Estas funciones son además de dominio público.

---

[22] Ibíd.

Lo que se denomina firma digital es un mensaje resumido mediante una función Hash y cifrado con una clave privada. Este es el esquema de firma digital mediante una función Hash:



Fuente: MORENO. Ob. cit.

Su mecanismo es el siguiente:

- El emisor aplica al documento una función Hash conocida, con lo que obtiene un resumen Hash.
- Encripta el resumen con su clave privada.
- Envía al receptor el documento original plano y el resumen Hash cifrado.
- El receptor B aplica la función Hash al resumen sin cifrar y desencripta el resumen cifrado con la clave pública de A.
- Si los resúmenes coinciden existirá la seguridad de que A ha sido el emisor del documento. Si no coinciden, B sabrá que no lo ha enviado A o que el documento ha sido interceptado durante el medio de envío y modificado. Si los resúmenes no coinciden es posible también que el mensaje haya sido alterado en su viaje desde A hasta B, hecho que invalida el documento.

Las funciones Hash y la firma digital son elementos indispensables para el establecimiento de canales seguros de comunicación, basados en los certificados digitales.

De acuerdo con Moreno, para que una función pueda considerarse Hash debe cumplir los siguientes requisitos:

- Transformar un texto de longitud variable en un bloque de longitud fija, que generalmente es pequeña (algunas son de 16 bits).
- Ser fácil de usar y de implementar.
- Ser irreversible, es decir, no se puede obtener el texto original de un resumen Hash.
- Ser imposible encontrar dos mensajes diferentes cuya firma digital mediante la función Hash sea la misma (es decir, no debe haber posibilidad de colisión entre mensajes).

Si se desea además mantener un intercambio de información con confidencialidad, basta con cifrar el documento a enviar con la clave pública del receptor.

Las *ABA Guidelines* describen el proceso de creación y verificación de una firma digital de la siguiente manera:

Creación de una firma digital. Como se aprecia en la figura 1, para firmar un documento cualquiera el signatario delimita el mensaje que será firmado. El mensaje delimitado es llamado el mensaje A. Luego, mediante la función Hash del *software* del signatario, computa un resultado Hash único (o resumen) para el Mensaje A. El *software* del signatario luego transforma el resultado Hash en una firma digital, empleando la clave privada del signatario.

Generalmente, una firma digital es adjuntada al mensaje y transmitida con el mensaje. Sin embargo, es posible que la firma sea enviada por separado, siempre y cuando mantenga una asociación indubitable con el mensaje.

Verificación de una firma digital. Como se aprecia en la figura 2, la verificación de una firma digital es llevada a cabo al computar un nuevo Hash del mensaje original, mediante la misma función Hash usada para crear la firma digital. Luego, empleando la clave pública del remitente y el nuevo resultado Hash, el verificador comprueba si la firma digital ha sido creada empleando la correspondiente clave privada y si el nuevo resultado Hash computado

Figura 1
Proceso de creación de firma digital

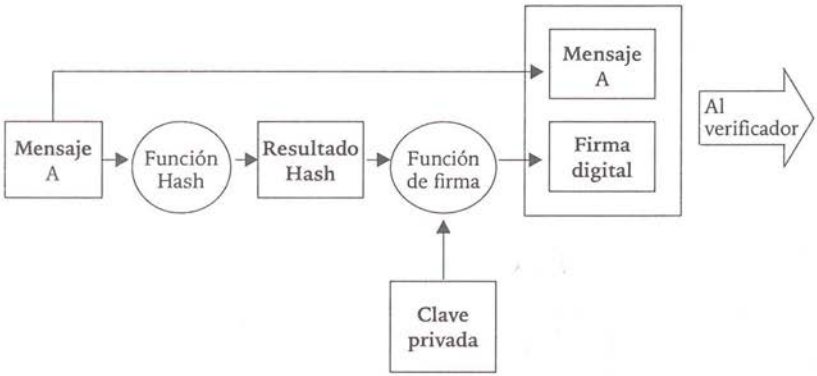
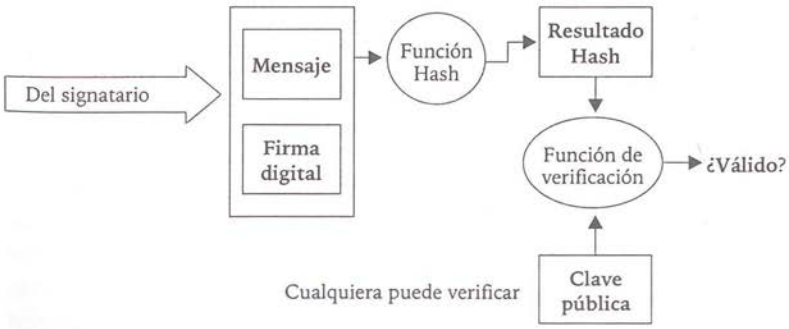


Figura 2
Proceso de verificación de la firma digital



coincide con el resultado Hash original que fue transformado en la firma digital durante el proceso de firma.

El *software* de verificación confirmará la firma digital como Mensaje A verificado si la clave privada del signatario fue empleada para firmar el mensaje digitalmente. Para comprobarlo es necesario constatar que la clave pública del signatario haya sido empleada para verificar la firma, porque la clave pública del signatario verificará solo una firma digital creada por la clave privada del signatario, que debe ser de su exclusivo dominio. Otro requisito para confirmar la firma digital es que el mensaje no haya sido alterado. Esto se comprueba si el resultado Hash computado por el verificador es idéntico al resultado Hash extraído de la firma digital durante el proceso de verificación.

2.9. *Public Key Infrastructure*

Hemos visto el funcionamiento de la firma digital y su vinculación con la criptografía. Las dos forman lo que se conoce como infraestructura de clave pública o *Public Key Infrastructure*. El PKI, según la definición en un documento de trabajo de la Microsoft Corporation, es «el conjunto de servicios del sistema operativo y de aplicaciones que facilitan el uso de la criptografía de claves públicas».[23] Según este documento de trabajo, un PKI permite:

Administrar claves. Una PKI facilita la emisión de claves nuevas. Además permite revisar o revocar claves existentes y administrar el grado de confianza que garantizan las claves de los distintos emisores.

Publicar claves. Ofrece una forma bien definida de que los clientes busquen y recuperen claves públicas y sepan si una clave

[23] Microsoft Corporation. «Introducción a la infraestructura de claves públicas de Windows 2000». En <http://www.microsoft.com/latam/technet/articulos/windows2k/pkiintro/>.

específica es válida o no. Sin la posibilidad de recuperar claves y averiguar si son válidas, los usuarios no pueden utilizar los servicios de claves públicas.

Usar claves. Una PKI proporciona una manera sencilla de utilizar las claves, no solo moviéndolas donde se necesiten sino, también, dando aplicaciones fáciles de usar que realicen las operaciones criptográficas de claves públicas. Esta utilidad aporta seguridad al correo electrónico, al comercio electrónico y a las redes.

Finalmente, debemos mencionar que el PKI permite el empleo de la firma digital y la criptografía, así como la comprobación de autenticidad de los mensajes de manera automática.

2.10. Conclusiones

1. La firma tradicional —es decir, la firma manuscrita— es la empleada inicialmente para cumplir las siguientes funciones: identificativa, declarativa, probatoria, identificadora y de autenticación.

2. La firma electrónica y la firma digital son las respuestas tecnológicas a las nuevas formas de realizar operaciones de comercio vía Internet (*e-commerce*). La diferencia entre ellas es de género (firma electrónica) y especie (firma digital). Tienen las mismas funciones que la firma manuscrita tradicional.

3. La firma digital es una firma electrónica que emplea el sistema de criptografía asimétrica para, principalmente, garantizar la identidad del autor de un mensaje y la integridad del mensaje.

4. Una firma digital debe permitir la identificación del signatario, solo debe poder generarla el emisor del documento, debe ser infalsificable e inimitable y debe permitir detectar la alteración de los mensajes. A diferencia de lo que sucede con la firma manuscrita, la misma persona puede ser titular de varias firmas digitales.

5. Jurídicamente, la firma digital es un medio de seguridad cuya función probatoria permite la identificación de una persona y de la autoría de un mensaje, además de la integridad del mensaje.

6. Los elementos de la firma digital son los datos de creación y de verificación de firma, y los dispositivos de creación y de verificación de firma.

7. El funcionamiento de la firma digital está vinculado a los siguientes elementos:

- La criptografía asimétrica o simétrica, que permite cifrar y descifrar los mensajes transmitidos vía Internet. Ella concierne a los temas de confidencialidad, autoría y no-repudiación de mensajes.
- La función Hash, que garantiza la integridad de los mensajes.

8. La firma digital, como un medio de seguridad jurídica en el comercio electrónico, permite solucionar los siguientes problemas:

- La identificación de las partes en una operación de comercio y de la autoría de los mensajes enviados mediante la criptografía asimétrica.
- La determinación de la integridad de los mensajes enviados por la red, con el objeto de realizar operaciones de comercio electrónico, por medio de la función Hash.
- La no-repudiación de los mensajes electrónicos, ya que con la criptografía asimétrica es posible determinar quién ha enviado el mensaje.
- La confidencialidad de la información transmitida por los sujetos participantes, ya sea por medio de la criptografía simétrica o de la asimétrica.

9. La firma digital, a pesar de permitir la solución de los problemas mencionados, tiene una limitación, que disminuye su eficacia como medio de seguridad jurídica. En efecto, como hemos visto, la firma digital es la asociación de dos claves, una pública y una privada, que son básicamente dos algoritmos o números que se obtienen con procedimientos matemáticos determinados. Sin embargo las claves, aisladamente, carecen de vinculación con el titular. Este hecho significa que no es posible garantizar fehacientemente que el titular de una firma digital es verdaderamente quien dice ser.

3. ENTIDADES DE CERTIFICACIÓN Y CERTIFICADOS DIGITALES

3.1. Introducción

Como hemos señalado en las conclusiones del punto anterior, las firmas digitales adolecen de una debilidad que atenúa su calidad de medio de seguridad jurídico para el comercio electrónico. Se trata de la imposibilidad de garantizar con el empleo mismo de la firma si su titular es quien dice ser.

Debido a que una de las características del *e-commerce* es la posibilidad de entablar relaciones con personas ubicadas en distintas partes del mundo, es imposible verificar la identidad de las personas que afirman ser titulares de una firma determinada cuando se encuentran en lugares distantes. Este problema no existiría si la esfera en la que se desenvuelve el *e-commerce* fuera reducida. En ese caso, sería factible comprobar la titularidad de las firmas digitales para verificar la identidad de sus titulares, y así evitar el problema de la repudiación de los mensajes.

Sin embargo, como hemos señalado en repetidas ocasiones, la esfera en la que se desarrolla el comercio electrónico es muy amplia, y tiene proyecciones de ampliarse cada vez más. En palabras de Martínez Nadal:

> No obstante, la utilización de firmas basadas en la criptografía asimétrica plantea el problema de la distribución fiable de las claves públicas. En efecto, cuando el destinatario de un mensaje firmado digitalmente desea proceder a su verificación, necesita tener acceso a la clave pública de la parte firmante con la seguridad de que se corresponde con la clave privada del mismo, *y con la seguridad de que efectivamente el firmante es quien dice ser* [...][24]

Sobre esta limitación de la firma digital la autora señala que «[...] una firma digital verificada con una clave pública únicamente garantiza que el mensaje ha sido firmado por el poseedor de la

[24] MARTÍNEZ NADAL. Ob. cit., p. 75. La cursiva es nuestra.

correspondiente clave privada; *pero no garantiza, por sí sola, la identidad del poseedor de la clave privada*».[25]

Por lo tanto, es imposible realizar una verificación directa de la titularidad de las firmas digitales. En efecto, sería demasiado costoso para un comerciante en Singapur verificar directamente la titularidad de la firma digital de un comerciante peruano.

Empleando conceptos vinculados con el análisis económico del derecho, los costos de transacción serían demasiado altos si no existiera la función de certificación, y ello excluiría el *e-commerce* como modalidad comercial.

En este punto se constata la necesidad de realizar una función de verificación, certificación o autenticación[26] de las partes participantes en una transacción de *e-commerce*, así como de los mensajes que transmiten. De estas se encargan las entidades de certificación. El objetivo de las entidades o autoridades de certificación, también llamadas terceras partes de confianza (*trusted third parties*), es asociar una persona determinada a una firma digital. Para lograrlo se valen de la emisión de los certificados digitales.

Se plantea un problema de identidad de las partes, pues, luego de la verificación de una firma digital con una clave pública, el destinatario de un mensaje puede estar seguro de que ha sido creada con la clave privada del emisor. Sin embargo, no puede estar seguro de si el emisor es quien dice ser, salvo que lo conozca personalmente. Como se puede apreciar, la firma digital actúa en un plano abstracto. Simplemente vincula una clave privada a una pública y viceversa. Las entidades de certificación, en cambio, actúan en un plano concreto, dinámico, al vincular una clave pública a su titular.

---

[25] Ibíd., p. 77. La cursiva es nuestra.

[26] De acuerdo con las ABA Guidelines, la función de autenticación es un proceso empleado para asegurar la identidad de una persona o la integridad de información específica. La autenticación de un mensaje involucra asegurar la fuente y que el mensaje no haya sido modificado o reemplazado en el transcurso de su tránsito de un emisor a su destinatario.

La función de certificación se vale de dos elementos: uno subjetivo, que está constituido por quienes realizan la actividad de certificación, es decir, las entidades de certificación; y uno objetivo, constituido por los certificados digitales. A continuación analizaremos con mayor detalle los dos elementos de la función de certificación, considerándola un medio de seguridad jurídica de vital importancia para el comercio electrónico.

3.2. Entidades de certificación

3.2.1. Definición de entidad de certificación

Para Martínez Nadal,

> Tercera parte de confianza (*Trusted Third Party* o TTP) es cualquier entidad de confianza de las partes intervinientes en una transacción para proporcionar servicios de seguridad; aquella específica tercera parte de confianza que desempeña de forma fundamental la función de emisión de certificados se conoce, entre otras expresiones, como autoridad de certificación, entidad de certificación, proveedor o prestador de servicios de certificación o simplemente certificador [...][27]

Según Ramos Suárez, la autoridad de certificación es «[e]sa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Actuaría como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información».[28]

Estas definiciones son suficientes para determinar que una entidad de certificación es básicamente una tercera parte, ajena a los sujetos del comercio electrónico, que cumple una función de

---

[27] MARTÍNEZ NADAL. Ob. cit., p. 78.

[28] RAMOS SUÁREZ, Fernando. «Cómo aplicar la nueva normativa sobre firma electrónica». En <http://www.vlex.com>.

identificación. Sin embargo, consideramos conveniente realizar ciertas precisiones.

En primer lugar, respecto a su denominación, consideramos que el término correcto es «entidades de certificación». No consideramos apropiada la denominación «autoridades de certificación», ya que ese nombre evoca la idea de una autoridad administrativa del Estado que desempeña la actividad de certificación. Como indicaremos más adelante, las entidades de certificación pueden ser personas de derecho público o privado. Por lo tanto, la actividad puede estar a cargo del sector público o del privado.

En segundo lugar, se podría interpretar que las entidades de certificación realizan una función pública,[29] que es desempeñada únicamente por el Estado. Sin embargo, no consideramos que sea una función desempeñada solo por el Estado exclusivamente. Las entidades de certificación pueden ser personas de derecho privado; es más, consideramos que la función de certificación debe ser realizada por el sector privado principalmente. La razón es que el sector privado, a diferencia del público, es más flexible a los cambios e innovaciones en todo tipo de ámbito, y con mayor razón en el campo del comercio y de la tecnología.

En tercer lugar, somos de la opinión de que las entidades de certificación no son un sujeto más del comercio electrónico, aunque se les llame terceras partes de confianza. Las entidades de certificación son un medio al cual recurren las partes en una operación de comercio electrónico para otorgar seguridad jurídica a sus transacciones.

---

[29] Sobre la función pública de las entidades de certificación afirma Jijena Leiva: «La trascendencia pública de su función pasa por el hecho de que cuando certifican dígitos o algoritmos y la pertenencia de esos dígitos a personas concretas y determinadas por sus características propias, están ejerciendo la potestad jurídica de otorgar «Fe Pública» en el marco de las transacciones comerciales». JIJENA LEIVA, Renato. «Firma digital y entidades certificadoras. Regulación legal en la administración pública chilena». En <http://publicaciones.derecho.org/redi/No._35_-_Junio_del_2001/2>.

3.2.2. *Características de las entidades de certificación*

- *Son un medio de seguridad jurídica en el comercio electrónico.*

Como hemos indicado, las entidades de certificación son un medio de seguridad del cual se valen los sujetos participantes en una operación de comercio electrónico para garantizar la identidad de las partes.

Sería imposible, desde nuestro punto de vista, considerar estas entidades como otros sujetos que intervienen en el *e-commerce*, ya que no podrían ser al mismo tiempo un medio y un sujeto de esta actividad.

- *Certifican la identidad de quien interviene en una operación de comercio electrónico.*

Una de las conclusiones a las que llegamos con referencia a la firma digital es que no puede garantizar la identidad de una persona que se identifique con una clave privada en un esquema de criptografía asimétrica. En otras palabras, las dos claves (privada y pública) están íntimamente ligadas entre sí, pero no con el titular de la firma digital.

Como afirma Barzallo, «[u]na de las principales limitaciones que presenta la firma electrónica en la actualidad es la autenticidad de la identificación representada en la firma electrónica, ya que los bits que llegan con la firma electrónica no tienen relación propia con las claves del firmante».[30]

Como indica el autor, no existe una asociación entre el firmante y su clave pública, es decir, es imposible asegurar la identidad del titular de una firma digital únicamente con su clave pública.

- *Complementan la función de la firma digital como medio de seguridad jurídica.*
- *Debido a que la función de la firma digital como medio de seguridad jurídica tiene la limitación que hemos señalado, las entidades de certificación*

[30] BARZALLO, José Luis. «Los terceros de confianza en el comercio electrónico». En <http://vlex.com/redi/No._33_-_Abril_del_2001/8>.

complementan esta función dando fe de la asociación entre la clave pública y la identidad de su titular.

- *Cumplen una función pública.*

Las entidades de certificación cumplen, a nuestro parecer, una función pública, ya que certifican la identidad de una persona frente a cualquier tercero que tenga intenciones de vincularse jurídicamente con ella. Por lo tanto, la certificación determina un efecto vinculante para el titular de la firma digital que sea certificada.

Esta función es vital para el desarrollo del comercio electrónico, pues será el elemento generador de confianza en el sistema y, por lo tanto, incentivará su crecimiento. Por estas razones, consideramos que la función de certificación es de carácter público, al margen de quién sea la entidad encargada del servicio.

3.2.3. Funciones de las entidades de certificación

Según Muñoz Esquivel, las entidades de certificación tienen las siguientes funciones:

- Principalmente, garantizar el principio de equivalencia funcional[31] de los mensajes electrónicos de datos frente a los documentos tradicionales o en papel
- Las entidades de certificación mantienen un registro y un estampado cronológico en la transmisión y en la recepción de los mensajes de datos, hecho que permite verificar que un mensaje

[31] El principio de equivalencia funcional establece que los actos y contratos suscritos por medios de firma electrónica tienen la misma validez y producen iguales efectos que los celebrados por escrito y en papel. Este principio se vale de las siguientes presunciones. En primer lugar, se reputarán como escritos estos actos y contratos cuando la ley exija que consten por escrito. En segundo lugar, la firma digital se considerará como firma manuscrita para todos los efectos legales. Este principio, sin embargo, no se aplicará a los actos que por ley requieran de una formalidad que no pueda ser cumplida por medios electrónicos. Extraído de GONZÁLEZ OGAZ, Cristóbal. «Algunos aspectos sobre el proyecto chileno de ley sobre firma electrónica y los servicios de certificación de firma electrónica». En <http://vlex.com/redi/No._35_-_Junio_del_2001/9>.

de datos ha sido efectivamente enviado por su emisor y recibido por su destinatario.[32]

Para Barzallo esta es la importancia de las entidades de certificación:

- La figura de la entidad de certificación evita el rechazo de una oferta aceptada y perfeccionada como contrato de acuerdo con la legislación que regule el acto mercantil o civil.
- Genera confianza y permite identificar y verificar la existencia de los actos realizados.
- Permite conocer la identidad de las partes de un acto jurídico.[33]

Respecto de las funciones de las entidades de certificación afirma Jijena Leiva:

> Junto con las medidas técnicas de resguardo y certeza provistas por la criptografía para disponer de un entorno seguro en relación con la autenticación electrónica, y porque las firmas digitales van más allá que la mera encriptación que sólo asegura la confidencialidad de un documento, jurídicamente se ha regulado la existencia de entidades que certifiquen —generando los bits necesarios para hacerlo— y publiciten las firmas digitales que se usen o, dicho de otro modo, que en un proceso de validación *autentifiquen la identidad de los emisores y receptores* que envían o reciben los mensajes firmados, cuyos antecedentes personales o nominativos además registran o archivan. Así, al lograrse que el receptor de un mensaje sepa indubitablemente que el emisor del mismo es realmente quien dice ser y que éste, a su vez, posteriormente *no pueda negar el envío,* se alcanzan *mayores grados de confianza en las relaciones comerciales* electrónicas o virtuales.[34]

---

[32] MUÑOZ ESQUIVEL, Oliver. «Actividad de las entidades de certificación frente a la función notarial». En <http://vlex.com/redi/No._35_-_Junio_del_2001/15>.

[33] BARZALLO. Ob. cit.

[34] JIJENA LEIVA, Renato. «Firma digital y entidades certificadoras. Regulación legal en la administración pública chilena». En <http://publicaciones.derecho.org/redi/ No._35_-_Junio_del_2001/2>. La cursiva es nuestra.

Según Viega Rodríguez, estas son las funciones de la autoridad certificadora:

- Publicar las claves públicas
- Realizar la identificación física antes de entregar las claves y luego controlar si la clave pública pertenece a la persona que dice ser su titular
- Certificar el procedimiento de identificación
- Publicar toda situación de suspensión, revocación, extinción o modificación de la clave pública[35]

A partir de lo que afirman estos autores concluimos que las entidades de certificación tienen las siguientes funciones:

- *Garantizar el principio de equivalencia funcional*

De acuerdo con este principio, como hemos señalado, se pretende otorgar a los actos firmados con una firma digital los mismos efectos que le otorgaría una firma manuscrita.

Una de las funciones de la firma manuscrita es la identificación de las personas que firman un documento. Al no garantizar la firma digital la identificación fidedigna de su titular, las entidades de certificación cumplen con este cometido y permiten que el principio de equivalencia funcional tenga vigencia y aplicación.

- *Identificar a las partes en la celebración de un acto jurídico*

La identificación de las partes, al autentificar la identidad de los emisores y receptores de los mensajes firmados, es posible mediante la asociación de una clave pública —y por consiguiente, de una firma digital— a su titular. En virtud de esta asociación, las entidades de certificación permiten la indubitable identificación de los participantes en la celebración de un acto de comercio llevado a cabo por medio de la firma digital.

---

[35] VIEGA RODRÍGUEZ, María José. «La firma digital y la autoridad certificante en Uruguay». En <http://www.alfa-redi.org/revista/revista.asp?idRevista=49>.

- *Evitar el rechazo de una oferta aceptada y perfeccionada como contrato de acuerdo con la legislación que regule el acto mercantil o civil*

Al hacer posible la identificación del firmante de un documento, es posible evitar que este niegue su autoría. Por lo tanto, se logrará solucionar el problema de la repudiación de los mensajes en el comercio electrónico.

- *Generar confianza e identificar y verificar la existencia de los actos realizados*

Alcanzar mayores grados de confianza en las relaciones comerciales es una función agregada de las entidades de certificación. Esta función no es exclusiva ni excluyente de los demás medios de seguridad jurídica del *e-commerce,* debido a que las transacciones concluidas por medio de una firma digital, y acreditadas por una entidad de certificación, tendrán validez jurídica y vincularán a sus titulares. Por lo tanto, las obligaciones contraídas por este medio serán exigibles. Se logra de esta manera una función agregada, no propiamente jurídica: incentivar el aumento de las transacciones comerciales concretadas con una firma digital.

- *Certificar el procedimiento de certificación de la identidad del titular de una clave pública*

Esta función es una de las más importantes, puesto que de su correcta aplicación dependerá que la función de certificación cumpla su papel como medio de seguridad jurídica.

- *Mantener un registro de las claves públicas y de sus titulares*

Con un registro se logra distribuir las claves públicas. En otras palabras, se publicita a los titulares de firmas digitales, hecho que estimula el crecimiento del comercio electrónico y, particularmente, el uso de la firma digital.

Aun cuando hemos mencionado varias de las funciones de las entidades de certificación, compartimos la opinión de Martínez Nadal, quien considera que su función fundamental es la asociativa, es decir, la capacidad de vincular a una persona con su clave pública. Esta posibilidad le garantiza al destinatario de un mensaje firmado digitalmente que el mensaje fue firmado con la clave privada del emisor y que el emisor es quien dice ser. Citamos a la autora:

> Ante la necesidad de una forma de distribución segura de las claves públicas [...], la solución técnica ofrecida consiste en la intervención de una o más terceras partes de confianza que emiten certificados que, a la vez que sirven para distribuir la clave pública, *sirven de forma fundamental* para asociar, de forma segura, la identidad de una persona concreta a una clave pública determinada [...] La principal función del certificado es asociar la identidad de una persona determinada a una clave pública concreta (e indirectamente a una clave privada) [...][36]

Algunas de las funciones señaladas serán tratadas nuevamente en los puntos relativos a la operatividad de las entidades de certificación.

3.2.4. Funcionamiento de las entidades de certificación

- Requisitos para su funcionamiento
  - *Autorización previa*

Un tema muy debatido respecto de los requisitos de funcionamiento de las entidades de certificación es si deben contar con la autorización previa de alguna entidad del Estado. Toda opción tiene ventajas y desventajas, y, cualquiera que sea la elección, se tratará de un tema de opción legislativa.

Una de las ventajas de contar con un sistema de autorización previa es que está garantizado un mínimo nivel de calidad en la prestación de servicios de certificación. Esta garantía, como hemos señalado, es básica para asegurar que este medio de seguridad cumpla con su objetivo. Como afirma Martínez Nadal, «[e]l sistema de autorización, acreditación o licencia, en efecto, establece un sistema regulador mínimo para proporcionar un nivel básico de confianza en las prácticas de la entidad certificadora».[37]

Sobre la misma ventaja afirma Barzallo:

> Supone que se han cumplido ciertos requisitos exigidos que le otorgan credibilidad a la entidad de certificación, ya que los requisitos no solo estarán mencionados, sino que habrá una autorización (certificación)

---

[36] MARTÍNEZ NADAL. Ob. cit., p. 78 y 79. La cursiva es nuestra.

[37] Ibíd., p. 137.

> que declare que la empresa obtentora de la autorización cumple con los requisitos exigidos por la ley. Para esto se presume la buena reputación y seriedad del organismo público encargado de fungir como autoridad de certificación.[38]

Sin embargo, tenemos una objeción, ya que de alguna manera este sistema requiere de la buena reputación y de la seriedad del organismo público que está a cargo de dar la autorización, y es denominador común, al menos en los países latinoamericanos, el desprestigio y la lentitud del aparato estatal.

Otra ventaja radica en la estandarización de los servicios de certificación. Como hemos señalado, el ámbito en el cual se desenvuelve el comercio electrónico es muy extenso y promete expandirse con el tiempo. Esta tendencia implica la necesidad de contar con sistemas estandarizados que permitan el intercambio de mensajes desde el lugar donde estén las partes, siempre y cuando tengan la tecnología adecuada. A propósito afirma Martínez Nadal:

> [...] uno de los principales problemas legales para el desarrollo del comercio electrónico viene dado por la existencia de distintas regulaciones legales divergentes (o la falta de ellas) y, en concreto, la falta de exigencias comunes para las entidades de certificación; ello puede plantear serios obstáculos para la confianza transfronteriza en un comercio como el electrónico desarrollado por encima de barreras interestatales.[39]

Frente a estas ventajas se presenta el sistema de la libre competencia, según el cual las entidades de certificación no requieren de una autorización para operar. Los aspectos positivos de este sistema son su flexibilidad y su capacidad de adaptarse a nuevas modalidades de comercio y a los avances tecnológicos. La tecnología, como hemos indicado, avanza mucho más rápido que el Derecho, y, por lo tanto, se debe permitir la flexibilidad de ciertas figuras jurídicas. Por ello, el sistema de libre competencia sería adecuado.

---

[38] BARZALLO. Ob. cit.

[39] MARTÍNEZ NADAL. Ob. cit., p. 138.

Este sistema pone en evidencia las desventajas del sistema de la autorización previa. En efecto, este sistema no es capaz de adaptarse con rapidez a los cambios en los hábitos de comercio y a la aparición de nuevas tecnologías, ya que la burocracia estatal se lo impide.

La función de certificación, que como hemos indicado es una función pública, no se verá afectada, ya que no requiere de autorización previa. En la actualidad, un sustituto del respaldo del Estado para garantizar la efectividad y la eficiencia en la prestación de un servicio es el prestigio que un prestador de servicios de certificación pueda tener en el mercado. En efecto, en nuestra sociedad, basada en una economía de mercado y de libre competencia, los diversos agentes económicos tienen entre sus más importantes activos lo que se llama *prestigio comercial*: la calidad en la prestación de servicios y la atención debida al cliente. Estos valores, agregados a un servicio determinado, en realidad no son meros valores agregados sino el servicio en sí mismo, que es lo que permite un adecuado posicionamiento en el mercado. Por este motivo, el soporte estatal para garantizar la prestación de un servicio puede ser reemplazado por el cuidado que deberá tener un prestador de servicios de certificación en sus actividades. En efecto, de no tenerlo no será competitivo y quedará excluido del mercado. En otras palabras, un incentivo para que las entidades de certificación presten adecuadamente sus servicios es la posibilidad de que pierdan su prestigio si no lo hacen. No se trata de un incentivo jurídico sino, más bien, comercial.

Somos de la opinión de que debe existir un sistema mixto, en el cual coexistan los dos sistemas descritos. De esta manera, será el propio mercado el que decidirá si acudirá a un prestador de servicios previamente autorizado por el Estado o a uno que no tenga esta autorización. Sin embargo, se debe precisar que, aun cuando no exista una aprobación previa para el funcionamiento de las entidades de certificación, será indispensable que cumplan con ciertos requisitos básicos para garantizar un nivel mínimo de calidad. Al respecto afirma Barzallo:

> El sistema que debe imperar es uno mixto, es decir, semiregulado, que conjugue características de voluntariedad y de autorización, sin que los beneficios de uno u otro sistema puedan considerar su aplicación injusta o irreal.
>
> Este sistema funciona estableciendo requisitos mínimos que deben ser cumplidos por las entidades de certificación que quieran emitir certificados. Estos requisitos de los certificados serán adaptados al sistema jurídico al cual se pretenda aplicar y se tomarán requisitos basados en estándares internacionales mínimos sin los cuales la función de certificación pierde su valor. Entonces será necesario contar con un sistema permanente de consulta, así como de revocación y la seguridad en la emisión de los certificados debe ser completa.
>
> Estos requisitos mínimos no buscan obstaculizar el establecimiento de entidades de certificación que tengan las condiciones necesarias para ejercer sus funciones de confianza.[40]

En conclusión, lo que propone es una autorización voluntaria por parte del Estado. Esta autorización —en realidad, reconocimiento— tendría un valor agregado. Como afirma Martínez Nadal,

> [...] se considera que sería útil que los proveedores de servicios de certificación dispusieran de sistemas de acreditación voluntaria, que ofrecen mayor seguridad, para ganarse la confianza de los consumidores. Si el mercado demanda tales sistemas, se concluye, el resultado será una mayor seguridad jurídica tanto para el proveedor de servicios como para el consumidor.[41]

- **Obligaciones de las entidades de certificación**

Tomamos como referencia las obligaciones establecidas en el real decreto ley.

Comprobación de identidad y otros datos personales de los solicitantes de certificados

Dentro de las obligaciones de las entidades de certificación, esta es una de las más importantes. En efecto, es la base de la función de

---

[40] BARZALLO. Ob. cit.

[41] MARTÍNEZ NADAL. Ob. cit., p. 143.

certificación, pues asegura la identidad de la persona que emplea una firma digital para cifrar un mensaje. En torno a esta obligación surgen cuestiones relevantes que analizaremos a continuación.

Métodos de comprobación de la identidad

Entre los métodos con los que una entidad de certificación puede verificar la identidad del solicitante de un certificado digital están los siguientes:

- Requerimiento de la presencia física

Se trata de un método tradicional para asegurar la identidad de una persona. En nuestra opinión es altamente seguro. Además, permite comprobar la capacidad del solicitante y su voluntad de solicitar el certificado.

- Documentos acreditativos

Una entidad de certificación puede ser menos rigurosa en su verificación de la identidad de una persona y limitarse a exigir ciertos documentos acreditativos para confirmar la identidad del solicitante, sin la necesidad de la presencia física. Aunque se trata de un método más flexible, es regularmente seguro. Sin embargo, es el único aplicable en el caso de las personas jurídicas a las cuales no se les puede exigir la presencia física.

Los documentos que puede exigir la entidad de certificación son el original del documento de identificación (o en su defecto una copia legalizada por notario público), una solicitud con firma legalizada por notario público, los documentos que acrediten la constitución de la persona jurídica y los poderes debidamente registrados del representante, en caso de que el solicitante sea una persona jurídica o actúe en representación de otra persona natural.

- Confirmación de datos personales por una tercera parte

En este caso, una tercera parte cumple el mismo papel que las entidades de certificación pero en una esfera diferente, ya que verifica la información proporcionada por el solicitante. Este método se puede emplear cuando la entidad de certificación esté muy lejos del lugar donde reside el solicitante, hecho que hace imposible

cumplir la exigencia de la presencia personal o de los documentos acreditativos.

Debemos señalar que estos métodos serán adaptados por cada entidad de certificación de acuerdo a sus propias políticas de funcionamiento. No se puede exigir a ninguna un método en particular.

Atributos dinámicos

Ciertos datos de la identificación de un solicitante pueden variar muy eventualmente, como el estado civil, el nombre, el domicilio y la capacidad, entre otros. Hay otros datos, sin embargo, que pueden variar constantemente, como la representación que una persona puede ejercer en favor de otra. Estos datos sujetos a variación constante son conocidos como *atributos dinámicos*. Se debe exigir a las entidades de certificación la comprobación de las circunstancias personales de los solicitantes de los certificados que sean relevantes.

En consecuencia, los certificados que emitan estas entidades pueden contener información relativa a títulos académicos, el poder de representación del solicitante o su condición de administrador de una sociedad. En estos casos, la labor de las entidades de certificación se complica. En efecto, el hecho de que varíen constantemente dificulta la verificación de estos atributos dinámicos.

Por ello, consideramos que se debe exigir esta obligación de verificación solo cuando se presenta la solicitud y se otorga el certificado digital. Para mantener actualizados los atributos dinámicos en el certificado será necesario que el titular notifique cualquier variación a la entidad de certificación. Sin embargo, aun con esta solución se podrían presentar dos problemas, entre otros menos graves.

El primer problema que puede surgir es que un atributo dinámico (por ejemplo, un poder de representación) sea revocado, y que la revocación se haya inscrito en los registros públicos pero no en el registro de certificados. En este caso, si antes de celebrar un contrato electrónicamente con el titular una persona verifica en el registro de certificados digitales los atributos que figuran en el certificado, tendrá la certeza de que posee este atributo dinámico,

aunque haya sido revocado y la revocación se haya inscrito en los registros públicos.

Frente a este problema planteamos dos soluciones. La primera es establecer una conexión entre la entidad de certificación y los registros públicos, de manera que cualquier variación de los atributos dinámicos que se inscriba en registros sea comunicada a la entidad para que proceda, de ser el caso, a modificar el contenido del certificado o a revocarlo. La segunda es establecer un sistema de responsabilidad para el titular del certificado, obligándolo a notificar a la entidad de certificación cualquier cambio de los atributos dinámicos que figuran en el certificado. De esta manera, si incumple esta obligación, será responsable de los daños y perjuicios.

El otro problema que puede surgir es el inverso, es decir, que se revoque el certificado digital en el que consta la representación, pero que la revocación no se inscriba en los registros públicos. Si este hecho ocurre, una persona que ha celebrado un contrato electrónico con el titular del certificado revocado podría argumentar la ignorancia de la revocación del poder, que no ha sido inscrita en registros públicos, y, por lo tanto, actuar de acuerdo con los atributos que figuran como vigentes. Sin embargo, toda persona que pretenda celebrar un contrato con el titular de un certificado deberá comprobar su vigencia. Por lo tanto, no podría argumentar que desconoce lo que no ha sido inscrito en registros públicos. Con esto, el problema quedaría zanjado.

Intervención de entidades de registro locales

Como hemos señalado, la esfera del comercio electrónico es muy amplia. Este hecho puede limitar el campo de acción de las entidades de certificación, pues no podrán verificar la identidad de los solicitantes que se encuentren en lugares lejanos.

Por este motivo, las entidades de certificación se pueden valer de terceras entidades, que actúen en nombre y por cuenta de las primeras. Se trata de las entidades de registro local, entidades de registro o agentes de registro, y su función es servir de intermediarias entre los solicitantes de certificados y las entidades de certificación. Esta

posibilidad permite aplicar el método de la presencia física para comprobar la identidad de los solicitantes.

Es importante señalar que los agentes de registro no emiten certificados digitales. Esta función es exclusiva de las entidades de certificación. Las funciones que los agentes de registro pueden cumplir son las siguientes:

- Registro, baja y cambios de los atributos de los titulares
- Identificación de los titulares
- Autorización de solicitudes de emisión de certificados, de generación de claves y de recuperación de claves
- Aceptación y autorización de las peticiones de suspensión o revocación de certificados

Se deberá establecer los requisitos que los agentes de registro deberán cumplir para su funcionamiento, puesto que tienen, como hemos visto, una de las obligaciones más importantes dentro de la función de certificación.

Puesta a disposición del signatario de los dispositivos de firma digital

Las entidades de certificación deberán ofrecer a sus clientes el *software* o el *hardware* necesario para aplicar la clave privada, a fin de crear la firma y la clave pública necesarias para la verificación. Sin embargo, consideramos que, más que una obligación, se trata de una facultad de las entidades de certificación. De esta manera, podrían no solo prestar el servicio de emisión de certificados sino, también, vender bienes (*software* y *hardware*). Si se tratara de una obligación, se les estaría imponiendo una actividad que podría no ser de su interés.

Prohibición de copia o almacenamiento de datos de creación de firma

Los datos de creación de firma son, como hemos indicado, las claves privadas que se emplean para cifrar mensajes. Por ello, las entidades de certificación están obligadas a no almacenar ni copiar claves privadas, ya que se pondría en riesgo su exclusividad.

Como señalamos en relación a los datos de creación de firma, existen dos sistemas de generación de claves:

- Sistema o entorno del titular del par de claves

En este sistema el par de claves es generado con el mismo sistema del titular del certificado (posiblemente el mismo *hardware* y *software*) en el que la clave privada será almacenada y usada, con lo que se elimina el problema de transferencia segura de la clave.

La ventaja de este sistema es que solo el titular ha tenido acceso a la clave privada. Esta posibilidad genera una mayor confianza en torno a las claves privadas. Sin embargo, la desventaja reside en la fiabilidad del *hardware* y el *software* empleados en la generación de la clave. En efecto, si los mecanismos no son seguros, surgirá el problema de la generación de claves no fiables.

- Sistema central

El par de claves es generado en un sistema central de una tercera entidad, que puede estar asociada a la entidad de certificación. La clave debe ser transportada de un modo seguro al sistema del titular, para luego destruir la información relativa a la creación del par de claves y, sobre todo, la propia clave privada.

La ventaja que ofrece el sistema central es la opuesta a la desventaja que ofrece el anterior sistema, es decir, garantiza la emisión de claves de mayor calidad. La desventaja es el posible empleo fraudulento de las claves, en caso de que sean almacenadas o copiadas por la entidad de certificación o terceros.

¿Cuál de los dos sistemas es el que finalmente se debe aplicar? Consideramos que se debe permitir el empleo de ambos y que son los titulares quienes deberán decidir por cual optar. Sin embargo, nosotros elegiríamos el sistema central, puesto que la emisión de certificados de alta calidad es muy importante. Además, la desventaja del sistema central se puede superar adoptando medidas de seguridad.

Información previa a la emisión del certificado

Esta obligación está relacionada con la protección al consumidor, puesto que antes de la emisión la entidad de certificación

deberá informar el precio del servicio, las condiciones de empleo del certificado, sus limitaciones y la forma en que se garantiza su eventual responsabilidad, en caso de que se produzca algún daño por el incumplimiento de sus obligaciones.

Mantenimiento de un registro de certificados

Mantener un registro actualizado de los certificados, que incluyan determinada información referente al titular, les permitirá a los terceros que pretendan vincularse por medios electrónicos con algún titular verificar los atributos que dice tener.

Mediante esta obligación se cumple asimismo una función de publicidad de los certificados. De la misma manera, se puede tratar de un sistema de distribución de claves públicas. Por ejemplo, el destinatario de un mensaje cifrado que carece de la clave pública de su emisor podría acudir al registro de certificados para obtener la clave pública necesaria para descifrar el mensaje. Del mismo modo se publicitará los certificados que no tengan vigencia para que los terceros tengan conocimiento de ello.

Comunicación en caso de cese de actividad

El objeto de esta obligación es permitir que el titular de un certificado pueda contactar otro proveedor de servicios de certificación con la debida anticipación, para no obstaculizar el tráfico comercial.

Indicación de fecha y hora de expedición, y de revocación de un certificado

Los certificados digitales cumplen también una función probatoria, por lo que resultarán importante en el ámbito del comercio electrónico, pues un certificado vincula a una persona con su clave privada y con su clave pública. En muchas situaciones, será necesario determinar el momento exacto de una acción (la transmisión, creación o recepción de un documento, o el momento en que se realiza una declaración de voluntad).

En consecuencia, será necesario conocer el momento exacto en que se expidió o revocó un certificado, para determinar la eficacia de los actos llevados a cabo en virtud del contenido de un certificado.

Frente a esta obligación, la solución tecnológica la da el sello temporal digital. Sellar temporalmente un documento electrónico significa sellar temporalmente los datos que contiene, de forma que sea imposible cambiar un solo dato sin que el cambio no sea evidente. Como afirma Martínez Nadal:

> Por lo tanto, *los servicios de sellado temporal digital* capaces de confirmar el momento exacto de determinadas acciones son necesarios para dar fiabilidad y seguridad al sistema de certificados: si el certificado de una clave pública es cancelado porque la correspondiente clave privada ha sido puesta en peligro, una firma electrónica previamente creada con la mencionada clave privada mantendrá su valor sin duda alguna si un sello temporal independiente hubiera sido puesto antes de la cancelación del certificado.[42]

Fiabilidad de los servicios

Para que los servicios de certificación puedan ser considerados fiables se deberá tomar en cuenta lo siguiente, según afirma Barzallo:

> Otros requisitos importantes:
> - Características técnicas: contar con sistemas seguros para la creación, la revocación, cancelación y suspensión de certificados.
> - Personal competente: el personal debe ser calificado o con la experiencia necesaria para cumplir con las funciones que le corresponda.
> - Garantía: deberá tener el respaldo económico necesario para asegurar a sus clientes que responderá por cualquier incumplimiento de sus obligaciones.
> - Información de respaldo: esta información es importante por los archivos que debe mantener una entidad de certificación respecto de los certificados que hubiera emitido.
> - Mantener planes de control que eviten perjuicios por la cesación de sus actividades.
> - Infraestructura necesaria para verificar los datos de los certificados. En muchos casos no solo se trata de una confrontación de los datos proporcionados con las bases de datos de la entidad de certificación, sino que es necesario abrir entidades de certificación locales que se

[42] MARTÍNEZ NADAL. Ibíd., p. 209. La cursiva es nuestra.

> encarguen de verificar directamente los datos proporcionados, como la identidad o la representación que ostenta el titular del certificado. En estos casos, la entidad de certificación local se excluye de emitir certificados y cumple únicamente funciones de registro, verificación, la suspensión y cancelación de certificados.[43]

3.2.5. Niveles de certificación

Así como los titulares de las firmas digitales requieren de una certificación de identidad, las entidades de certificación necesitarán una certificación que las acredite. Si las entidades de certificación acreditan la identidad de los titulares de firmas digitales, ¿quién certifica las entidades?

La respuesta la tenemos en lo que se conoce como niveles de certificación. Existen dos niveles en la función de certificación. En el primer nivel, se encuentran las entidades que certifican la existencia e identidad de los prestadores de servicios de certificación de la identidad de los titulares de firmas digitales. En el segundo nivel, están las entidades que certifican la identidad de los titulares de firmas digitales.

En nuestra opinión, solo la función de certificación del primer nivel puede ser llevada a cabo por el sector público, ya que para este nivel se requiere de un mayor respaldo y certeza para certificar a los certificadores. Se puede implementar esta función de certificación mediante un registro de entidades de certificación.

Al respecto señala Jijena Leiva:

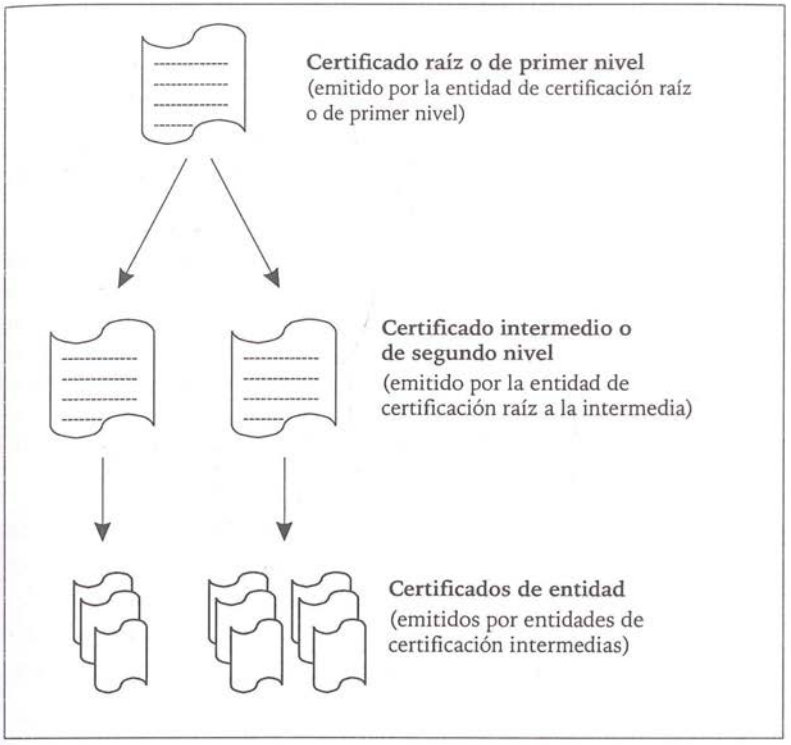
> Es necesario dar un paso más en la cadena [de certificación] y llegar al primer nivel de la misma. Porque las personas jurídicas que presten servicios de entidades certificadoras a su vez también deben ser certificadas, o dicho de otra forma, porque la infraestructura de firma digital o el sistema que la regule tiene que posibilitar que también las llaves públicas de dichas entidades certificadoras [de segundo nivel] puedan ser conocidas de forma segura por los suscriptores o signatarios que requieran de sus servicios, de manera tal que ellos sepan fehacientemente que

[43] BARZALLO. Ob. cit.

ha sido una tercera parte confiable la que emitió un certificado válido y vigente, o dicho de otra forma, la que otorgó fe pública en el marco de una operación de comercio electrónico. [44]

El gráfico nos muestra el funcionamiento de esta jerarquía.

Apariencia de una jerarquía de certificados



De acuerdo con los niveles de certificación existirán tres tipos de certificados: certificados de raíz, cuyo titular es la entidad de certificación de primer nivel; certificados intermedios, emitidos

[44] JIJENA LEIVA. Ob. cit.

por la entidad de certificación de primer nivel a las de segundo nivel; y certificados de entidad, emitidos por la entidad de certificación de segundo nivel a los titulares de firma digital.

3.2.6. Naturaleza jurídica de las entidades de certificación

Por último, una vez analizados los principales aspectos de las entidades de certificación, determinaremos su naturaleza jurídica.

Una de las cuestiones en debate respecto de estas entidades es determinar si la función de certificación debe ser llevada a cabo por el sector público o por el privado, es decir, si debe ser el Estado, los particulares o ambos quienes deban prestar los servicios de certificación.

Señala Barzallo, respecto al origen del problema en la determinación de la naturaleza jurídica de las entidades de certificación:

> Considero que parte del problema viene del nombre con el cual ha sido traducida del inglés esta figura de vital importancia para el comercio electrónico. Se traduce como AUTORIDAD DE CERTIFICACIÓN o en inglés CERTIFICATION AUTHORITIES, cuando el término adecuado a traducirse es Trusted Third Parties. La palabra Autoridad en el sistema romano tiene una implicación pública, esto es, sus actividades están orientadas al beneficio público y por ende se someten a los principios del derecho público.

Coincidimos con el autor citado en cuanto a la denominación de las personas que prestan el servicio de certificación. Por ello, hemos optado por denominarlas entidades de certificación.

Según Muñoz Esquivel existen tres teorías o corrientes que determinan a cargo de quién debe estar la función de certificación y, por ende, cuál es su naturaleza jurídica:

> **Teoría publicista: servicio público que busca la preservación de la fe pública**
>
> De acuerdo al autor chileno Renato Jijena Leiva, la existencia de las entidades de certificación en el marco del comercio electrónico obedece a la necesidad de un mecanismo de resguarde del principio jurídico de «fe pública».
>
> Parafraseando al jurista uruguayo Couture, Jijena Leiva define el principio de «fe pública» como la calidad particular de ciertos documentos que

consiste —o depende— no sólo en *la autoridad moral y técnica* de quien los ha elaborado, sino también en una ficción legal de que lo aseverado por una entidad facultada para hacerlo es verdad. Desde esta perspectiva, la función de las entidades de certificación se asemeja a la función fedal otorgada a los notarios públicos [...]. Sin embargo, el mismo autor reconoce que sería un gran error encomendar el trabajo de otorgar certificados digitales a entidades o funcionarios auxiliares de la administración de justicia como los notarios, que apenas manejan procesadores de textos o programas de bases de datos o de informática registral.

Postura privatista: actividad privada sujeta a las reglas del mercado
Esta postura sostiene que la actividad de las entidades de certificación no ha de estar sujeta a autorización previa por parte del Estado. Por el contrario, las mismas se rigen simplemente por las reglas del mercado, esto es, con base en un régimen de libre competencia. [...]

Postura ecléctica: servicio técnico reglamentado por el Estado
[...] Y es que en vez de otorgar una categoría jurídica específica a la actividad certificadora, dicha postura reconoce simplemente su semejanza con la función notarial, destacando su importante contenido técnico. Sin embargo, dicha postura refleja en sí misma una marcada tendencia publicista por cuanto permite que la función certificadora sea reglamentada por el Estado.[45]

De las corrientes mencionadas nos adscribimos a la última, es decir, a la ecléctica, ya que no se puede negar la función pública que realizan las entidades de certificación. En efecto, incluso se las ha comparado con los notarios públicos. Sin embargo, nos parece apropiado matizar la postura ecléctica con la privatista, pues no podemos dejar de tomar en cuenta las ventajas que se obtienen con la flexibilidad de las reglas del mercado. Sin embargo, al ser de vital importancia esta función pública, es necesario que se regulen los requisitos que las entidades de certificación deberán reunir para poder cumplir con ella y otorgar las garantías necesarias, sin que esta regulación implique una autorización previa para su funcionamiento.

---

[45] MUÑOZ ESQUIVEL. Ob. cit. La cursiva es nuestra.

Nuestra posición respecto de la función pública de las entidades de certificación concuerda con lo que afirma Jijena Leiva:

> La trascendencia pública de su función pasa por el hecho de que cuando certifican dígitos o algoritmos y la pertenencia de esos dígitos a personas concretas y determinadas por sus características propias están ejerciendo la potestad jurídica de otorgar «fe pública» en el marco de las transacciones comerciales.[46]

En conclusión, respecto de la naturaleza jurídica de la función de certificación podemos decir que es una función pública mediante la cual se da fe de la identidad del titular de una clave privada. Esta función es llevada a cabo por las entidades de certificación, que pueden ser personas de derecho privado o público, que constituyen una tercera parte que acredita la identidad de las personas que se pretenden vincular jurídicamente valiéndose de medios electrónicos. En este sentido, estas utilidades hacen las veces de un notario público.

3.3. Certificado digital

3.3.1. Definición de certificado digital

El certificado digital es el elemento objetivo de la función de certificación. Es el documento que da fe de la identidad del titular de una firma digital y de sus claves, tanto la pública como la privada.

Según Ramos Suárez:

> Los certificados digitales son registros electrónicos que atestiguan que una clave pública pertenece a un determinado individuo o entidad. Permiten verificar que una clave pública pertenece a una determinada persona. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro.[47]

---

[46] JIJENA LEIVA. Ob. cit.

[47] RAMOS SUÁREZ. Ob. cit.

De acuerdo con las *ABA Guidelines*, un certificado digital es

> Un mensaje que por lo menos:
> - Identifica a la entidad de certificación que lo emite.
> - Designa o identifica a su subscriptor.
> - Contiene la clave pública de su subscriptor.
> - Identifica su período operacional.
> - Está digitalmente firmado por la entidad de certificación que lo emite.

Debemos indicar que en la legislación española y en ciertos grupos de doctrina se realiza una distinción entre certificados reconocidos y no reconocidos.[48] Para los fines de nuestro estudio no realizaremos esta distinción, por lo que cualquier mención a los certificados digitales se referirá a los certificados que tienen plenos efectos jurídicos.

3.3.2. Características del certificado digital

- Es un documento electrónico. Es generado con medios electrónicos y tiene la validez de un documento escrito.
- Es expedido únicamente por entidades de certificación.
- Debe contener determinada información para que sea considerado un certificado digital. En otras palabras, es un documento que debe cumplir con determinadas formalidades.
- Además de la información que debe contener, puede contener otro tipo de datos relativos al titular de una firma digital, que, como hemos señalado, puede tener diversos fines. Por lo tanto, los certificados digitales también pueden tener diversos fines y ser de distintas clases.

---

[48] La diferencia radica en que los certificados reconocidos reúnen formalidades de las que carecen los certificados comunes. Por esta razón, a los primeros se les reconoce plenos efectos jurídicos. Consideramos que esta diferenciación no debe ser incorporada en una norma jurídica que regule los certificados digitales, ya que podría ser motivo de confusiones y complicaciones. En una ley o reglamento se deberían regular únicamente los certificados que tengan plenos efectos jurídicos.

- Tiene un período de vigencia previamente establecido, por lo que se deduce que su vigencia es limitada. Sin embargo, puede dejar de tener vigencia antes que se venza el período preestablecido cuando se produzcan los casos de revocación o de suspensión que más adelante estudiaremos.

Al respecto señala Martínez Nadal: «[...] dada la vida necesariamente limitada de las claves criptográficas desde el punto de vista técnico,[49] el certificado relativo a esas claves debe tener igualmente una vida limitada, finalizada la cual, debe dejar de confiarse en el mismo».[50]

La razón de la vida limitada de los certificados es, como hemos indicado, la necesaria vida limitada de una firma digital. Afirma Martínez Nadal que

> [...] el juego de clave pública y privada no debe considerarse válido para siempre; en un sistema gestionado de forma adecuada, cualquier juego de claves debería tener una vida limitada:
> - Para controlar las oportunidades de criptoanálisis, porque en efecto, el riesgo de ruptura del par de claves es mayor por la mayor exposición frente a terceros.
> - [...] para reducir el período de vulnerabilidad en que las claves podrían resultar comprometidas.
> - [...] para evitar el desfase técnico, la degradación de la calidad de la clave por el simple paso del tiempo.
> - [...] la existencia de certificados de vida breve hará más fácil la extinción y el cese de actividades de la entidad de certificación.[51]

---

[49] La autora señala que debido la rápida evolución de la tecnología, la seguridad de una firma digital puede ser prontamente violada. Por este motivo, la firma no puede tener una vida ilimitada, pues mientras más prolongada sea su validez, será más susceptible a ser violada.

[50] MARTÍNEZ NADAL. Ob. cit., p. 91.

[51] Ibíd., p. 102.

3.3.3. Funciones del certificado digital

- Verificar que una clave pública pertenece a una determinada persona. En consecuencia, procurar evitar que una persona utilice una clave haciéndose pasar por otra. Afirma Ramos Suárez al respecto: «[...] 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».[52]
- De esta manera se trata de solucionar el problema de la identidad de las personas en el *e-commerce*. En palabras de Martínez Nadal: «[...] la función básica de los certificados y el elemento clave de tal función: *la comprobación de la identidad* del firmante [...]».[53]
- Publicar la clave pública del emisor de un mensaje. Como señalaremos más adelante, el certificado digital debe contener la clave pública del emisor del mensaje. Por lo tanto, es un medio para dar a conocer la clave pública de una persona.
- Publicar la clave pública de la entidad de certificación. El certificado digital deberá contener la clave pública de la entidad de certificación, ya que el certificado es firmado digitalmente por la entidad y debe ser descifrado por el destinatario del mensaje. Para hacerlo, requerirá de la clave pública de la entidad de certificación.
- Función probatoria. En el certificado digital consta la información relativa a la identificación del titular de una firma digital, y sus atributos dinámicos —en caso de existir— en un momento determinado. Los certificados digitales tienen entonces una función probatoria de la identidad del titular de una firma digital y de los atributos dinámicos que pudiera tener en un momento determinado. Esta información es oponible a terceras personas.

---

[52] RAMOS SUÁREZ. Ob. cit.

[53] MARTÍNEZ NADAL. Ob. cit., p. 80. La cursiva es nuestra.

3.3.4. Contenido del certificado digital

De acuerdo con las definiciones citadas, y tomando como base las disposiciones del real decreto ley, tenemos que el contenido de los certificados digitales es el siguiente:

- *La indicación de que se expiden como tales*

Esta exigencia tiene el fin de identificar al certificado como tal, cualquiera sea la forma que pueda adoptar, o cualquiera sea el medio tecnológico por el cual se genere. De esta manera se está en correspondencia con el principio de neutralidad tecnológica.

- *El código de identificación único del certificado*

De esta manera se podrá identificar los distintos certificados que una entidad de certificación pueda expedir. En caso de que una persona tenga diversos certificados, sea en una entidad de certificación o en varias, no serán confundidos.

- *La identificación del prestador de servicios de identificación que expide el certificado*

Es preciso que la identidad de la tercera parte de confianza que da fe de la identidad del titular de una firma digital sea plenamente identificada. En esto se basa el sistema de confianza requerido para la realización de una operación de comercio electrónico. Por ello, las entidades de certificación son a su vez acreditadas por las entidades de certificación de primer nivel.

Se deberá señalar, entre otra información, el nombre o razón social de la entidad de certificación, su domicilio, su dirección de correo electrónico, su registro único de contribuyente e información registral.

- *La firma electrónica del prestador de servicios de identificación*

El certificado digital, al igual que el mensaje cifrado que será enviado, deberá ser cifrado digitalmente para salvaguardar su integridad. Por ello, la entidad de certificación deberá firmarlo digitalmente. De este modo, complementariamente, se tendrá la certeza de que la entidad es la que efectivamente firmó el documento.

- *La identificación del signatario*

Debido a que el certificado tiene como fin principal acreditar la identidad del titular de una firma digital, debe contener los datos de identificación del titular.

Se deberá consignar los nombres y apellidos completos del signatario, el número de su documento de identificación, su domicilio, su dirección de correo electrónico y cualquier otra información que resulte relevante.

En la legislación española se ha permitido que el signatario se identifique con un seudónimo si no desea revelar su verdadero nombre al vincularse utilizando medios electrónicos, aun cuando la entidad de certificación sí conozca su identidad.

Respecto a esta posibilidad consideramos que no debería permitirse en el caso de los certificados que tengan plenos efectos jurídicos, ya que su función principal es la de identificar indubitablemente al titular de una firma digital. Esta utilidad sería imposible si se identifica con un seudónimo, pues sería muy difícil requerirle el cumplimiento de las obligaciones contraídas o que asuma la responsabilidad por eventuales daños ocasionados.

- *Los datos de verificación de firma que correspondan con los datos de creación de firma que estén bajo control del signatario*

El certificado debe contener la clave pública del signatario, para que el destinatario de un mensaje pueda descifrar el mensaje cifrado con la clave privada del signatario. Como indicamos, esta exigencia permitirá la publicidad de claves públicas.

- *El comienzo y el fin del período de validez del certificado*

Como hemos señalado, el certificado digital tiene una vida limitada, por lo que deberá indicar su período de vigencia.

- *Los casos de representación*

En caso de que en el certificado se incluyan atributos dinámicos, como son los supuestos de representación, se deberá hacer referencia al documento en el que consta la representación que ejerce el titular del certificado. Pero se debe tener en cuenta que, al tratarse de atributos dinámicos, se podrá dar fe de su existencia antes de su emisión, no después.

- *Los límites del uso del certificado*

En el certificado se podrá consignar las limitaciones para su empleo como las restricciones respecto de los tipos de operaciones comerciales o las personas a las se dirige un mensaje cifrado digitalmente. También se podrá establecer límites en cuanto a la cuantía de las transacciones para las cuales se pueda utilizar el certificado.

3.3.5. Clases de certificados digitales

Según José Cuervo, las entidades de certificación pueden emitir los siguientes tipos de certificados:

- Certificados de identidad: son los más utilizados actualmente dentro de los *criptosistemas* de clave pública y ligan una clave pública a una identidad personal (usuario) o digital (equipo, *software*, etc.).
- Certificados de autorización o potestad: certifican atributos no relacionados con la identidad del usuario como, por ejemplo, la representación que pueda ejercer a favor de otra persona.
- Certificados transaccionales: atestiguan que un hecho o una formalidad acaecieron o fueron presenciados por un tercero.
- Certificados de tiempo o estampillado digital: permiten dar fe de que un documento existía en un instante determinado.[54]

Ramos Suárez concuerda con algunos de los tipos de certificados que una entidad de certificación puede emitir:

- Certificados de identificación: identifican y conectan un nombre a una clave pública.
- Certificados de autorización: ofrecen otro tipo de información relacionada con el usuario, como la dirección comercial, antecedentes, catálogos de productos, etc.

---

[54] Cuervo. Ob. cit.

- Otros certificados colocan a la autoridad certificadora en el rol de notario, por lo que se pueden utilizar para dar fe de la validez de un hecho o de que un hecho efectivamente ha ocurrido.
- Otros certificados permiten determinar día y hora en que el documento fue digitalmente firmado (*digital time-stamp certificates*).[55]

Nos adscribimos, sin embargo, a la tipología de certificados de José Cuervo.

3.3.6. Vigencia de los certificados digitales

Teniendo en cuenta la importancia de la determinación exacta de la vigencia de los certificados, estudiaremos el tema con mayor profundidad.

Las *ABA Guidelines* señalan, respecto de la vigencia de los certificados, que

> El período operacional —o de vigencia— de un certificado empieza en la fecha y hora en la cual es emitido por la entidad de certificación (o en una fecha y hora posteriores si es que en el certificado es así establecido), y termina en la fecha y hora en la cual expira, o cuando anticipadamente sea revocado o suspendido.

En cuanto a la vigencia de los certificados digitales, su inicio es de fácil determinación. No sucede lo mismo con el fin de la vigencia, pues pueden darse diversos casos.

La finalización definitiva del período de vigencia del certificado puede producirse por dos motivos: por la finalización del plazo de vigencia previsto en el propio certificado o por la pérdida de vigencia anticipada por causas no previstas, ya sea por la suspensión o por la revocación del certificado. Mediante la revocación de los certificados se produce la pérdida definitiva e irreversible de su vigencia. La suspensión, en cambio, implica la pérdida temporal de la eficacia del certificado digital.

---

[55] RAMOS SUÁREZ. Ob. cit.

Dicho en otras palabras, la interrupción de la vigencia de los certificados digitales puede darse de dos maneras: definitiva, por la expiración ordinaria o por las causales de revocación específicas, o temporal, debida a la suspensión de los certificados digitales.

Respecto de la pérdida de vigencia de los certificados, es necesario que los terceros puedan conocer la extinción del certificado. De ahí se deriva que sea necesario establecer procedimientos para publicitarlo.

- **Causas de la pérdida de eficacia definitiva**

Expiración ordinaria del certificado por causas previstas o expiración del período de validez

La verificación de esta causal implica que el período de vida del certificado digital ha transcurrido sin la ocurrencia de circunstancias extraordinarias. Se pueden establecer las causales de expiración ordinaria del certificado. Respecto de esta posibilidad no existen limitaciones. Se puede, por lo tanto, prever que el certificado expirará transcurrido un lapso de tiempo determinado o por el acontecimiento de un hecho determinado.

Cualquiera que sea la causa estipulada de expiración ordinaria deberá ser lo suficientemente clara y específica para que no haya ambigüedad respecto de la determinación de sus alcances.

Invalidez anticipada

Los siguientes son los casos de invalidez anticipada de los certificados digitales. En estos casos, el certificado pierde su validez antes de que se venza el período de vigencia previamente establecido.

- *Revocación por el signatario*

Este caso implica la decisión del titular del certificado de acortar el período de vigencia antes del plazo inicialmente establecido. Deberá solicitarlo a la entidad de certificación con la adecuada anticipación, a fin de otorgarle el tiempo necesario para que el certificado que va a ser revocado pierda vigencia a partir del momento que se crea conveniente solicitar.

No solo el titular del certificado puede solicitar la revocación. También pueden hacerlo, en ciertos casos, otras personas, como el representado a quien se revoca la representación que se le ha otorgado.

- *Pérdida o inutilización por daños del soporte del certificado*

En el caso del titular del certificado, esta circunstancia puede ocurrir si se pierde o daña la tarjeta inteligente a la que está incorporado o el disco duro de su computadora. En el caso de las entidades de certificación, la invalidez anticipada puede deberse a la pérdida o el daño del soporte en que almacena los certificados. En ambos casos, lo que se pretende proteger es la pérdida de la clave pública del titular.

- *Utilización indebida por un tercero*

Este caso se refiere a la utilización no autorizada de la clave privada del titular. Será el propio titular quien deberá solicitar la revocación.

- *Resolución judicial o administrativa que lo ordene*

La revocación del certificado en este caso se realizará automáticamente en la fecha en que la correspondiente autoridad lo disponga. No es necesaria la comunicación previa al titular ni mucho menos su autorización.

Consideramos que deberá ser una entidad del Estado la que disponga la revocación del certificado. Deberá asegurar la notificación de la correspondiente disposición a las entidades de certificación de primer nivel, para que procedan a notificar a las entidades de segundo nivel.

- *Fallecimiento del signatario o de su representado*

En este caso, se plantea la duda de quién debe solicitar la revocación del certificado, porque hasta que no se le comunique a la entidad de certificación ni se notifique la situación no tendrá como tener conocimiento de la revocación. Este aspecto es importante, ya que la revocación se tendrá como eficaz solo si es inscrita en el registro de certificados.

En el caso de extinción de personas jurídicas, existe un proceso constituido por una serie de etapas que concluye en la inscripción de la extinción en los registros públicos. No se puede considerar extinguida a la persona jurídica hasta que la inscripción se efectúe.

Sin embargo, consideramos que el certificado de una persona jurídica deberá ser revocado al iniciarse su proceso de extinción, y no esperar hasta que la extinción se inscriba en los registros públicos, ya que existirá un lapso —desde el inicio de la extinción hasta su inscripción— en el cual existirá un certificado cuyos atributos no serán exactos.

- *Cese en las actividades del prestador de servicios de certificación*

Para este supuesto existen dos alternativas: la transferencia de los certificados a otra entidad de certificación, con el previo consentimiento del titular del certificado, y, si la transferencia no es posible, la extinción anticipada del certificado.

- *Inexactitudes graves en los datos aportados por el signatario para la obtención del certificado*

Este hecho ocurre cuando el certificado digital se ha generado con datos inexactos, falsos o incorrectos. En caso de que estos datos afecten la correcta identificación del sujeto, por causas que se le puedan imputar, el certificado deberá ser revocado de oficio por la entidad de certificación. Este no es el caso cuando la inexactitud de los datos es imputable a una mala actuación de la entidad.

- *Eficacia de la pérdida de vigencia del certificado*

La extinción del certificado digital es oponible frente a terceros por dos razones:

- *Causas de eficacia inmediata*

Estas causas pueden ser dos: el fin del período de validez del certificado, es decir, la extinción ordinaria, o el cese de las actividades de la entidad de certificación, salvo que, previo consentimiento del signatario, se transfieran los certificados a otra entidad.

- *Causas de eficacia diferida a la publicación en el registro de certificados*

Son todas las que no han sido mencionadas para las causas de extinción inmediata. Se trata de la revocación por el signatario, la pérdida o inutilización por daños del soporte del certificado, la utilización indebida por un tercero, la resolución judicial o administrativa que lo ordene, el fallecimiento del signatario o de su representado, o inexactitudes graves en los datos aportados por el signatario para la obtención del certificado.

- **Causas de pérdida de vigencia temporal**

Puede darse el caso de que el titular de un certificado o la entidad de certificación no quieran revocar el certificado, dado el carácter irreversible y permanente de la revocación. Frente a esta circunstancia, se contempla la figura de la suspensión temporal de los certificados. Sin embargo, los terceros deberán ser notificados, por lo que la suspensión deberá ser publicada en el registro de certificados digitales.

La suspensión del certificado requerirá de un procedimiento, al igual que la revocación. La suspensión podrá ser solicitada por el titular del certificado, por su representado, por la propia entidad o por la autoridad administrativa o judicial.

Respecto de la suspensión de los certificados, las *ABA Guidelines* manifiestan que «[a] menos que el contrato establezca otra cosa, la entidad de certificación debe suspender un certificado tan pronto como sea posible tras la petición de una persona de la que la entidad crea razonablemente que es el suscriptor o la persona autorizada». Por último, se deberá establecer claramente el período de duración de la suspensión.

3.3.7. Equivalencia de certificados digitales

Debido a que el medio en el cual se desenvuelve el comercio electrónico es muy amplio, es usual que participen en él personas que se encuentran en estados diferentes. Este hecho es un obstáculo para el funcionamiento de los certificados digitales, ya que es posible que los certificados emitidos en un país no sean reconocidos en otro. Esta circunstancia limita la función de identificación de los certificados digitales en un ámbito internacional.

Por esta razón, se deben crear mecanismos para que los certificados emitidos en un estado sean reconocidos en otro. Hay dos formas de hacer frente a este obstáculo: que el sector privado preste los servicios de certificación y que se establezca políticas de reconocimiento de certificados.

- **Prestación de servicios de certificación por el sector privado**

Como hemos señalado, si los servicios de certificación son prestados por el sector privado, no existirán barreras fronterizas o estatales para el reconocimiento de certificados emitidos por prestadores de servicios de certificación.

De esta manera, el reconocimiento del Estado para otorgar fiabilidad a los prestadores de servicios de certificación puede ser reemplazado por el prestigio que estos prestadores adquieran en el mercado. Este reconocimiento permitiría que un certificado digital emitido en un país por una entidad de certificación de prestigio mundial sea reconocido en cualquier otro. Por esta razón, afirmamos que en la prestación de servicios de certificación el sistema de libre competencia, junto con la teoría privatista, favorecería el reconocimiento de los certificados digitales.

- **Establecimiento de políticas de reconocimiento de certificados**

Otro de los mecanismos para lograr el reconocimiento de los certificados digitales es la adopción de políticas de reconocimiento de los certificados, en las cuales se determine claramente los estándares mínimos de los certificados digitales.

Esta medida implica la estructuración de un marco normativo internacional elaborado por el sector privado, no por el Estado, en el cual se regule las políticas de reconocimiento de los certificados digitales.[56]

La combinación de estos dos sistemas constituirá una medida eficaz y eficiente para el establecimiento de políticas de reconocimiento. Permitirá dejar de lado su dependencia de la voluntad del aparato estatal que, como hemos indicado, es lento y se adapta con dificultad a la evolución del comercio de acuerdo con las nuevas tecnologías.

---

[56] Estas políticas podrían ser elaboradas por la American Bar Association, por la UNCITRAL o por la Cámara de Comercio Internacional.

3.3.8. Naturaleza jurídica del certificado digital

La naturaleza jurídica del certificado digital está determinada por su función probatoria. Por esta razón, podemos afirmar que tiene la naturaleza jurídica de un medio de prueba, mediante el cual se evitan situaciones de incertidumbre respecto de la identidad y las facultades del titular de una firma digital.

Se trata, por lo tanto, de un medio de seguridad jurídica para las operaciones de comercio electrónico, al hacer oponibles a terceras personas la identidad y las atribuciones de los participantes en el *e-commerce*.

3.4. Conclusiones

1. En el comercio electrónico es muy importante que exista una función de certificación mediante la cual se permita fehacientemente la identificación de las partes participantes. La función de certificación se vale de dos elementos: uno subjetivo (las entidades de certificación) y uno objetivo (los certificados digitales).

2. La función más importante de las entidades de certificación es la función asociativa, es decir, su capacidad de vincular a una persona con su clave pública, de tal manera que el destinatario de un mensaje firmado digitalmente tenga la certeza no solo de que el mensaje fue firmado con la clave privada del emisor sino, también, de que el emisor es quien dice ser.

3. Se discute si la función de certificación debe estar a cargo del sector privado o del público. En el primer caso se postula un sistema de libre competencia (al cual nos adherimos) en el que no se requiere de autorización previa del Estado. En el segundo caso se postula el sistema de autorización previa, en el cual se requerirá de la autorización de un ente estatal para el funcionamiento de las entidades de certificación.

4. Las entidades de certificación tienen a su cargo determinadas obligaciones en la ejecución de la función de certificación. La principal obligación es la comprobación de la identidad del titular de

una firma digital y de otros datos personales de los solicitantes de los certificados.

5. Los certificados digitales puede contener información que puede variar constantemente, como la representación que una persona puede ejercer en favor de otra. Estos datos sujetos a variación constante se conocen como atributos dinámicos. Se debe exigir a las entidades de certificación la comprobación de todas las circunstancias personales relevantes de los solicitantes de los certificados en el momento en que un certificado sea solicitado y expedido.

6. Así como los titulares de las firmas digitales requieren de una certificación de su identidad, las entidades de certificación requerirán de una certificación que acredite su existencia e identidad ante los titulares de firmas digitales. Esta figura de la certificación de los certificadores es conocida como niveles de certificación. Existen dos niveles. En el primero están las entidades que certifican la identidad de los titulares de firmas digitales. En el segundo se encuentran las entidades que certifican la identidad de los prestadores de servicios de certificación.

7. En cuanto a la naturaleza jurídica de las entidades de certificación, son entidades que cumplen una función pública: dar fe de la identidad del titular de una clave privada. Constituyen una tercera parte acreditante de la identidad de las personas que pretendan vincularse jurídicamente valiéndose de medios electrónicos.

8. El certificado digital es el elemento objetivo de la función de certificación. Es su objeto material, un documento o mensaje en el cual constan los datos de identificación del titular de una firma digital, así como sus diversos atributos.

Existen diversas clases de certificados: los que certifican la identidad de una persona (certificados de identidad); los que certifican atributos que no se refieren a la identidad del usuario, como la representación que ejerce una persona a favor de otra (certificados de autorización o potestad); los que atestiguan que algún hecho o formalidad acaeció o fue presenciado por tercero (certificados transaccionales); y los que permiten dar fe de que un documento existía

en un instante determinado (certificados de tiempo o estampillado digital).

9. El período de vigencia es uno de los datos más importantes que debe contener un certificado digital para establecer desde y hasta cuándo la información que contiene es oponible a terceras personas. El período operacional o de vigencia de un certificado empieza en la fecha y en la hora en la que es emitido por la entidad de certificación (o en una fecha y una hora posteriores si el certificado es así establecido), y termina en la fecha y en la hora en la que expira, o cuando anticipadamente sea revocado o suspendido.

La vigencia de los certificados puede ser interrumpida de forma permanente (en el caso de la revocación) o de forma temporal (en caso de suspensión). Existen diversos supuestos de hecho que encajan dentro de una u otra forma de interrupción de la vigencia de los certificados.

10. La eficacia de los certificados digitales como un medio de seguridad jurídica internacional puede verse afectada si en un Estado no existen mecanismos para el reconocimiento de certificados emitidos en otro. Esto se puede resolver con la adopción del sistema de libre competencia para su funcionamiento y con el establecimiento de políticas de reconocimiento.

11. La naturaleza jurídica de los certificados digitales es la de un medio probatorio de la identidad y atributos del titular de una firma digital. De esta manera, constituye un medio de seguridad jurídica en el comercio electrónico.

4. LOS MEDIOS DE PAGO ELECTRÓNICOS

4.1. Introducción

Como hemos señalado, con la firma digital y los certificados digitales se garantiza la integridad y la confidencialidad de los mensajes y la identidad de las personas que se vinculan por medios electrónicos. Además, se evita la repudiación de los mensajes transmitidos en la red y, por consiguiente, se garantiza el cumplimiento de las obligaciones contraídas por medios electrónicos. Del mismo modo, existe

un respaldo jurídico respecto de las dos primeras fases del comercio electrónico: la localización de las partes y la contratación electrónica.

No obstante, no hemos indicado la forma en la que se cumplirá con las obligaciones contraídas en la etapa de ejecución. Es preciso estudiar a continuación los medios electrónicos de pago en el *e-commerce*.

Es necesario delimitar entonces el ámbito en el que encuadraremos nuestro estudio. Para ello debemos indicar que no todas las obligaciones contraídas por Internet se pagarán necesariamente por medios electrónicos. La forma de pago dependerá del tipo de obligaciones contraídas.

Por ejemplo, si se ordena una pizza a domicilio por Internet, la obligación de pago de la persona que ordene la pizza podrá ser realizada en el momento en que la pizza es entregada, es decir, personalmente. En este caso, el pago no se realizará por medios electrónicos.[57] Sin embargo, se puede pactar que la obligación de pago sea ejecutada en el mismo instante en que se realice la orden. En ese caso, el pago se deberá realizar electrónicamente.[58]

El vendedor de pizzas, en cambio, no podrá cumplir con la entrega de las pizzas por medios electrónicos, ya que no es posible el envío de una pizza por estos medios; al menos, hoy en día la tecnología no lo permite. Entonces será necesario que la entrega sea personal y con la utilización de un medio tradicional.

Se podría deducir de lo dicho que los compradores de bienes son los que tienen siempre la opción de pagar electrónicamente, a diferencia de los vendedores, al no ser posible el envío de bienes por medios electrónicos. Sin embargo, este hecho no es del todo cierto, ya que ciertos bienes sí pueden ser transmitidos por medios

---

[57] En este caso, estaremos frente a una operación de comercio electrónico indirecto, es decir, una operación en la que se realiza la contratación por medios electrónicos y se cancela con un medio no electrónico.

[58] En este caso, estaremos frente a una operación de comercio electrónico directo, en la que tanto la contratación como el pago se efectúan por medios electrónicos.

electrónicos. Es el caso de la venta de libros electrónicos, *software*, música o películas, entre otros bienes que pueden ser contenidos en soportes electrónicos.

En consecuencia, podemos afirmar que el empleo de medios electrónicos de pago en el comercio electrónico será posible en la medida en que los bienes que se haya acordado entregar para el pago de las obligaciones contraídas puedan ser transmitidos electrónicamente. Por lo tanto, este estudio comprenderá la entrega de bienes transmisibles por medios electrónicos para realizar el pago de obligaciones, es decir, las operaciones de comercio electrónico directo.

Empleando la terminología del Código Civil respecto de los tipos de obligaciones, podemos decir que el pago por medios electrónicos de obligaciones no comprenderá las obligaciones de hacer y no hacer sino las obligaciones de dar, en las que el elemento preponderante es la entrega de un bien.

Restringiremos aún más el ámbito de aplicación de este estudio. Existen diversos bienes transmisibles por medios electrónicos que pueden ser empleados para el pago de obligaciones. Nosotros nos referiremos a las obligaciones de dar una suma de dinero, no a otros bienes transmisibles electrónicamente.

La razón por la que excluimos bienes distintos del dinero es que en su caso se aplicarán los sistemas de seguridad antes mencionados, como la firma digital y los certificados digitales. Para el empleo del dinero en Internet, en cambio, existen sistemas específicos de seguridad que explicaremos a continuación.

4.2. Aspectos jurídicos del pago

Consideramos necesario explicar las implicancias jurídicas del pago en términos generales antes de empezar con el análisis de los medios de pago electrónicos.

4.2.1. Definición de pago

En palabras de Osterling y Castillo, el pago es, considerando su idoneidad, «[...] el medio ideal de extinción de las obligaciones. El

pago implica la ejecución de la obligación en las condiciones convenidas en su origen, vale decir, el cumplimiento dentro de los términos previstos. Pagar es actuar conforme a lo debido».[59] De esta definición se desprende que el pago implica la ejecución íntegra de una obligación para que quede extinguida.

Cabe precisar entonces en qué consiste la ejecución de estas prestaciones. En este sentido, afirman que «Pago, en Derecho de Obligaciones, es la ejecución de una prestación debida, ya sea ésta de dar, de hacer o de no hacer».[60] Esta definición concuerda con lo que afirmamos: que los pagos de obligaciones pueden ejecutarse de diversas maneras o, en otras palabras, mediante la ejecución de diversos tipos de prestaciones, como dar, hacer o no hacer.

Debemos señalar que este estudio está orientado a la realización de un pago mediante la ejecución de la prestación de dar una suma de dinero. Por lo tanto, cualquier referencia al pago que hagamos a continuación debe ser entendida como la ejecución de dar una suma de dinero.

4.2.2. Requisitos de pago

Para que el pago conlleve la extinción de una obligación deberá reunir los siguientes requisitos, según Osterling y Castillo:

- *Preexistencia de una obligación*

  Si el pago es considerado el medio para extinguir una obligación, si esta obligación no existe, la prestación debida no podrá tener la condición de pago.
- *Que la prestación se efectúe con* animus solvendi

  Este es un requisito de carácter subjetivo. Para considerar el pago como tal, será necesario que exista la intención del pago.

---

[59] Osterling Parodi, Felipe y Mario Castillo Freyre. *Tratado de las obligaciones*. Primera parte. Tomo IV. *Biblioteca para Leer el Código Civil*, Volumen XVI. Lima: Pontificia Universidad Católica del Perú, 1994, p. 134.

[60] Ibíd., p. 178.

- *Que se pague aquello que se debe*

Para que exista pago se deberá ejecutar la prestación acordada por las partes. En consecuencia, el acreedor no estará obligado a recibir una prestación diferente. En caso de aceptar esta prestación, se estará ante un mecanismo distinto de extinción de las obligaciones: la dación en pago. Por este motivo, para que el pago sea considerado como tal a fin de extinguir una obligación se deberá ejecutar la prestación convenida por las partes.

- *Que se pague íntegramente lo debido*

Para que el pago sea considerado como tal, por último, se deberá ejecutar la prestación debida íntegramente, es decir, en su totalidad, de modo que se extinga la vinculación entre un acreedor y un deudor. De este modo, quedará extinguida la obligación que los ataba. En caso de que la prestación no sea ejecutada en su totalidad, existirá aún un vínculo entre el acreedor y el deudor.[61]

4.2.3. Efectos del pago

El cumplimiento de la obligación de pago produce, como primer y principal efecto, la extinción de la obligación. Sin embargo, el pago no extingue de plano la obligación en todos los casos. En efecto, en muchas situaciones la obligación no se extingue, sino que se modifica. Este hecho sucede con el pago mediante una tarjeta electrónica de crédito, como veremos más adelante.

El segundo efecto que produce el cumplimiento de la obligación de pago por parte del comprador es el efecto liberatorio. Este implica que, el deudor queda liberado del poder coactivo del acreedor, de la sujeción jurídica.

Finalmente, el pago produce el efecto de satisfacción para el acreedor, en el sentido de que es cumplida la prestación debida. En líneas generales, el pago debe producir en forma simultánea los efectos indicados. Sin embargo, en determinadas ocasiones, la eficacia del pago no es total, circunstancia que justifica otro tipo de

[61] Ibíd., p. 182.

soluciones para la satisfacción del acreedor y la liberación del deudor. Estas soluciones se apartan un poco del esquema planteado y se dan precisamente en el caso del pago mediante tarjetas electrónicas.

4.2.4. Naturaleza jurídica del pago

Respecto de la naturaleza jurídica del pago existe un extremo desarrollo doctrinario. Nosotros seguimos en este punto a Osterling y Castillo, quienes afirman lo siguiente: «[...] debemos dejar establecido que el pago es un deber y un derecho. El deudor, al pagar cumple el deber que emane de la relación obligacional asumida. Pero no sólo tiene el deber de pagar. También tiene el derecho a hacerlo [...]».[62]

Como vemos, el pago es una institución jurídica compleja. No es solo un acto jurídico. Tampoco es simplemente un hecho jurídico, una obligación o un deber.

No siendo el presente trabajo uno abocado al pago, no profundizaremos más sobre este aspecto.

4.3. Medios de pago electrónicos

4.3.1. Definición de medios de pago electrónicos

Hemos mencionado brevemente los conceptos básicos de la institución jurídica del pago. A continuación estudiaremos la definición de los medios de pago electrónicos.

De acuerdo con el literal a) del artículo 2 de la recomendación 97-489-CE de la Comisión de las Comunidades Europeas del 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, estos son «[l]os instrumentos que permitan a su titular efectuar transferencias de fondos, realizar el retiro de dinero en efectivo, quedando dentro de esta definición los instrumentos de pago de acceso a distancia y los instrumentos de dinero electrónico».

---

[62] Ibíd., p. 134.

De acuerdo con esta recomendación, los instrumentos de pago de acceso a distancia son

> Instrumentos que permiten a su titular acceder a los fondos de su cuenta en una entidad, por el cual se autoriza el pago a un beneficiario, operación que normalmente exige un código de identificación personal o cualquier otra prueba similar de identidad. [Quedan incluidas, en particular, las tarjetas de pago (tarjetas de crédito, de débito) y los servicios de telebanco y de banca a domicilio].

Según la misma recomendación, los instrumentos de dinero electrónico son «instrumentos de pago recargable distintos de un instrumento de pago de acceso a distancia en los que se carga electrónicamente un valor».

Mariliana Rico Carrillo, respecto de los medios de pago electrónico, afirma que

> En un sentido general y amplio, los medios de pago electrónico no son más que los que comúnmente denominamos transferencias electrónicas de fondos (TEF), entendiendo por tales las transferencias de forma automática ejecutadas inmediata o simultáneamente a la orden dada por el titular de la cuenta bancaria por medio de un sistema electrónico.[63]

Complementamos estas definiciones con la nuestra: los medios de pago electrónicos son aquellos instrumentos que permiten extinguir una obligación —contraída o no por medios electrónicos— mediante la transferencia de fondos de propiedad del deudor a favor de su acreedor.

4.3.2. Características de los medios de pago electrónicos

De estas definiciones podemos inferir las siguientes características de los medios electrónicos de pago:

---

[63] RICO CARRILLO, Mariliana. «El pago mediante tarjetas en el comercio electrónico a través de Internet». Tesina presentada en la Universidad Carlos III de Madrid, en septiembre de 1999, para la obtención de la certificación de suficiencia investigadora, requisito para la obtención del título de doctor en derecho. Publicado en la *Revista de la contratación electrónica*, n.° 3, Universidad de Cádiz, marzo de 2000.

- *Permiten la extinción de obligaciones utilizando medios electrónicos*

El fin por excelencia de los medios de pago electrónicos es la extinción de obligaciones. Por lo tanto, estos medios recogen exactamente la finalidad del pago prevista en el Código Civil. La única diferencia radica en la forma de ejecutar el pago, es decir, en que el medio sea electrónico. Consideramos oportuno señalar que estos medios de pago pueden extinguir obligaciones contraídas por medios electrónicos y, asimismo, obligaciones contraídas por medios tradicionales

- *Son medios de pago íntimamente vinculados con la tecnología*

Como hemos indicado en el punto anterior, la única diferencia entre los medios de pago electrónicos y el pago regulado en el Código Civil radica en la forma en la que se ejecuta el pago. Por este motivo, los medios de pago electrónicos están ligados íntimamente a los avances tecnológicos. Existirán todos los medios de pago electrónicos que la tecnología desarrolle.

Es preciso señalar que el principio de neutralidad tecnológica es aplicable a los medios de pago electrónicos, es decir, mientras la tecnología desarrolle diversos mecanismos electrónicos para las transferencias de dinero o de fondos, estos mecanismos deberán considerarse medios de pago en tanto cumplan con la finalidad de extinguir las obligaciones. Por lo tanto, se les deberá aplicar las disposiciones legales referentes al pago.

- *Permiten un tráfico comercial fluido, al ser medios de pago de rápida ejecución*

Una de las ventajas de Internet es el ahorro de recursos, medidos tanto en dinero como en tiempo. Los medios de pago electrónicos no son la excepción a este valor agregado de Internet. En efecto, permiten que la extinción de obligaciones sea mucho más rápida y expeditiva. En cuestión de segundos es posible concretar una operación comercial y pagar obligaciones, no necesariamente contraídas por medios electrónicos.

- *Su mecanismo de funcionamiento es la transferencia de fondos del deudor a favor del acreedor*

El principio fundamental de funcionamiento de los medios de pago electrónico es la transferencia de fondos de un deudor a favor

de su acreedor. Los fondos pueden provenir de su cuenta corriente o de ahorros, de un monedero electrónico o de la transferencia de dinero electrónico. Todos estos medios de pago serán estudiados más adelante.

- *Requieren de mecanismos de seguridad eficientes*

Como toda aplicación que Internet ofrece, los medios de pago electrónico requieren de sistemas que garanticen el cumplimiento de su finalidad. Incluso los medios de pago electrónico requieren de un desarrollo especial de seguridades y garantías, pues se encuentra en riesgo la propiedad de los recursos que los sujetos que participan en el comercio electrónico emplean para operar económicamente mediante Internet.

En realidad, la custodia y la seguridad en el empleo de los medios electrónicos de pago están entre los aspectos más importantes del comercio electrónico. Sin duda son uno de los motivos por los que muchas personas no usan Internet para ejecutar operaciones comerciales. La posibilidad de que se extravíen recursos al emplear Internet es una variable constante que desalienta la práctica del *e-commerce*.

Al ser un aspecto medular en el comercio electrónico, la seguridad y la efectividad de los medios de pago electrónicos, requieren de un mecanismo de seguridad tan o más desarrollado que los mecanismos empleados para identificar y vincular jurídicamente a los sujetos del comercio electrónico. Dicho en otras palabras, ¿de qué vale garantizar la identificación fehaciente y la vinculación válida de los sujetos del comercio electrónico si no tienen mecanismos que les permitan efectuar el pago de sus obligaciones?

- *Constituyen por sí mismos un medio de seguridad en el comercio electrónico*

Consideramos, por lo tanto, que los medios de pago electrónicos son uno de los componentes del Sistema de Seguridad Jurídica en el Comercio Electrónico (SSJ).

4.3.3. Seguridad digital

Como hemos indicado, la seguridad en el empleo de los medios de pago electrónicos es indispensable. Por este motivo, ahondaremos en el tema de la seguridad digital en estos medios de pago.

■ Riesgos en el empleo de los medios de pago electrónicos

Sobre los posibles riesgos en el empleo del comercio electrónico en lo concerniente a los medios de pago, señala Gallegos que

> Los atacantes pueden robar el dinero codificado o los números de la tarjeta de crédito durante la transmisión y decodificar los números, y de esta manera usar, entonces, el dinero digital para comprar en Internet o usar esta información para obtener otra información valiosa o sensitiva. Por lo tanto, la seguridad del dinero digital debería dirigirse al proceso de transmisión.[64]

La encriptación sería una forma muy popular para proteger la información sensitiva durante la transferencia.

Para Gallegos, el riesgo principal que conlleva el uso de medios electrónicos es que terceros no autorizados accedan a la información que les permita disponer de estos medios y emplearlos sin autorización de su titular. Del mismo modo, considera que la encriptación es una posible solución pues, como hemos señalado, permite la transmisión de mensajes por la red de forma íntegra y confidencial.

Como vemos, el problema central de los medios de pago electrónicos es garantizar que la transferencia de fondos que se debe realizar para la ejecución del pago se lleve a cabo sin que terceras personas tengan acceso a la información transmitida (números de cuenta y claves de acceso, entre otros datos).

El mismo autor hace los siguientes comentarios con relación a la confidencialidad de la información y al control de acceso:

> **Confidencialidad**
> La confidencialidad de los servicios protege que la información no sea revelada o dada a conocer a grupos no autorizados. Más específicamente, protege a los datos transmitidos en la red. [...] Un servicio de confidencialidad de los datos hace factible la no inferencia a la información sensitiva desde el contenido o el tamaño de los ítems de los datos

---

[64] GALLEGOS, Frederick. «Preocupaciones sobre el control y la seguridad». En <http://www.isaca.org/percep/v2art3.htm>.

(por ejemplo, usando encriptación). Un servicio de confidencialidad del flujo de tráfico hace no factible que un extraño infiera la información sensitiva observando los flujos de tráfico de la red.

Control de acceso

El control de acceso es la capacidad para limitar o controlar el acceso a los sistemas host y a las aplicaciones por medio de enlaces de comunicaciones.

La meta del control de acceso está en proteger contra el acceso no autorizado a los recursos (por ejemplo, recursos de computación, recursos de comunicación o recursos de información).

El término acceso no autorizado incluye el uso, revelación, modificación, destrucción y emisión de comandos no autorizados.

Para lograr este control, cada entidad que trata de obtener acceso debe ser identificada o autenticada para que los derechos de acceso puedan ser adaptados al individuo.[65]

Como señala Gallegos, la confidencialidad de la información transmitida en la red (en el caso analizado, la información referida al empleo de medios de pago) es posible gracias a la encriptación, que permite, a su vez, controlar eficazmente el acceso a determinada información.

Nuevamente nos valemos de Gallegos para describir los tipos de amenazas que pueden surgir del empleo de medios electrónicos de pago:

Amenazas externas. Se originan fuera de un sistema.[66]

- **No intencional.** Desde organizaciones confiables o desde los adversarios [...] —que— podrían ser negligentes con la información o dañar

---

[65] Ibíd.

[66] Es preciso señalar que la referencia a la seguridad surge de la idea de un sistema de pagos efectuados en Internet. Para la ejecución de pagos por medios electrónicos se requiere de un sistema adecuado en el cual interactúen sujetos (banco, clientes, proveedores de bienes o servicios, entidades de certificación) e instrumentos (*software* adecuado, Internet). Por esta razón, la referencia a la seguridad implica el funcionamiento de este sistema de pagos.

o liberar información inconscientemente. Así, las amenazas externas pueden ser intencionales o no intencionales.

- **Las intencionales** pueden venir de info-terroristas, competidores o bromistas. Los info-terroristas quieren destruir los sistemas de información de dinero digital o las bases de datos porque perciben al sistema como una amenaza a su sistema de valor. Los competidores pueden buscar información que les dé una ventaja. Por lo tanto, el espionaje de los negocios trata de acceder a la información privada, así como a la de los clientes o números de cuenta.

Amenazas internas

Los sistemas son probablemente muy vulnerables a ser atacados desde adentro, especialmente por empleados deshonestos o descontentos que tienen autorización para acceder al sistema. Es difícil detectar cuando roban datos o dañan al sistema. Las amenazas no intencionales provienen de accidentes o de negligencia.[67]

Por último, Gallegos explica las posibles vulneraciones de seguridad en el empleo de medios de pago electrónicos:

Desde el momento en que se ingresan los números del dinero digital en una computadora hasta el momento que llega al último destino, pueden ser interceptados y leídos durante la transmisión. Esta, puede ser dividida en cinco pasos y cada uno de ellos tiene diferentes vulnerabilidades.

1. El dinero digital almacenado en la computadora del remitente: el dinero digital que usted crea[68] y envía a menudo es almacenado en su propia computadora o en el disco. Si se deja no encriptado, es vulnerable a ser comprometido por un «buscavidas» que tenga acceso a su computadora o disco.

2. En transmisión: la vulnerabilidad principal de este paso es la interferencia. Los atacantes pueden simplemente intervenir la línea, el cable de fibra óptica, y señales de satélite o microondas, que llevan la información sensitiva y el dinero digital.

---

[67] GALLEGOS. Ob. cit.

[68] Más adelante nos referiremos a la creación del dinero electrónico como medio de pago.

3. En el buzón de correo del receptor: una vez que el dinero digital es recibido, la transacción es almacenada en una porción de disco duro, es decir, un buzón del correo electrónico. Este puede estar en una computadora remota o en el disco duro del propio receptor. Se requiere de una contraseña para acceder a la transacción. Por lo tanto, es importante cifrar y manejar las contraseñas de forma de evitar que se conozcan.

4. Clasificado por el sistema de correo electrónico para propósitos administrativos: la mayoría de los sistemas de dinero digital purgarán todas las transacciones anteriores después de un tiempo especificado, pero también hacen copias de respaldo con propósito de facturación o en caso que falle el sistema. Si los atacantes acceden a estos archivos, una gran cantidad de información personal será revelada, incluyendo con quién usted se comunica, qué compra y dónde está.

5. Análisis del tráfico: aunque los atacantes no intercepten las transacciones, pueden aprender mucho sobre ellas haciendo un análisis del tráfico.[69]

■ Objetivos de la seguridad en el sistema de pagos electrónico

Para establecer los principales objetivos de la seguridad de los medios de pago electrónicos, nos valdremos de las afirmaciones de Gallegos:

Los objetivos de seguridad atienden a:

- Asegurar que cualquier servicio del sistema de dinero digital esté disponible a los usuarios cuando lo piden
- Asegurar la confidencialidad de la información del pago
- Asegurar la integridad de todos los datos de pago transmitidos por medio de las redes públicas
- Asegurar la autenticación del poseedor de la tarjeta de crédito de forma que sea el propietario legítimo de la cuenta
- Proveer la protección contra los ataques relacionados con el comercio electrónico
- Tener mecanismos separados de privacidad para el intercambio de la información general y el intercambio de datos de pago

[69] GALLEGOS. Ob. cit.

- Asegurar que cualquier servicio de sistema de dinero digital no sea degradado por factores como relámpagos, terremotos o inundaciones
- Asegurar que cualquier transacción, dinero digital o mensaje enviado llegue al destino apropiado
- Asegurar que cualquier dinero digital, transacción o mensaje recibido sea, exactamente, el que fue enviado (nada agregado o borrado)
- Controlar el acceso a las computadoras y otras partes conexas (esto significa terminales, *switches, módems, gateways, bridges, routers* e impresoras)
- Proteger la información en tránsito de ser vista, alterada o removida por una persona o dispositivo no autorizado
- Tener un plan de recuperación, si las vías de comunicación primarias y de respaldo fracasan.[70]

- **Consecuencias de la carencia de seguridad en los sistemas de pago electrónicos**

Una vez más recurrimos a lo que señala Gallegos sobre las consecuencias de la falta de seguridad en los sistemas de pago electrónicos.

> La carencia de un sistema de dinero digital seguro puede dar como resultado consecuencias serias para una compañía, incluyendo:
>
> - La destrucción de los datos
> - La exposición de la información y las fuentes propietarias
> - El acceso no autorizado a los recursos de la computadora
> - La pérdida de la confidencialidad y el secreto
> - La pérdida de la confianza del cliente
> - La negación de los servicios a los empleados y clientes
> - La pérdida de tiempo en la administración del sistema
> - Productos corrompidos o dañados enviados a los clientes
> - La información personal y financiera comprometida, dañada, destruida o alterada[71]

4.3.4. Naturaleza jurídica de los medios de pago electrónicos

Por las características señaladas, los medios de pago electrónicos son instrumentos a los cuales el Derecho ha otorgado un reconocimiento

---

[70] Ibíd.

[71] Ibíd.

jurídico para la extinción de obligaciones. Por lo tanto, configuran un medio de seguridad jurídica en el comercio electrónico que permite válidamente extinguir una obligación constituida al poder el deudor oponer su efecto extintorio contra su acreedor y contra los terceros que considere conveniente.

Podemos afirmar entonces que los medios de pago electrónico tienen una doble naturaleza jurídica: son un medio de extinción de obligaciones y, al mismo tiempo, un medio de seguridad jurídica en el comercio electrónico.

4.3.5. Clasificación de los medios de pago electrónicos

Nos valdremos de la clasificación de Mariano Maltese de los medios de pago,[72] con un fin únicamente ilustrativo. No pretendemos establecer esta clasificación como la única o la mejor.

La clasificación ha sido elaborada teniendo en cuenta el medio en el que se ejecuta el pago, es decir, Internet. Este criterio nos parece acertado, ya que, como hemos señalado, el soporte tecnológico del comercio electrónico es principalmente Internet, por lo que la ejecución de pago en esta actividad se realiza por esa vía. Por este motivo, una clasificación de los medios de pago electrónicos basada en el empleo de Internet nos parece apropiada, teniendo en cuenta la delimitación realizada en la introducción del tema que nos ocupa.

- *Medios de pago independientes*

Los medios de pago electrónicos independientes son aquellos que no requieren de Internet —al margen de que efectivamente la usen o no— para efectuar sus transacciones (por ejemplo, las tarjetas de crédito o ciertos monederos electrónicos).

---

[72] MALTESE, Mariano. «El pago electrónico en la Argentina - Diversos medios de pago relacionados con el comercio electrónico». En <http://vlex.com.ar/cn/Derecho_Inform@atico/12>.

- *Medios de pago dependientes parcialmente*

Los medios dependientes parcialmente son aquellos que necesitan de Internet pero solo en una etapa de su proceso (inicio, ejecución o término de la transacción).

- *Medios de pago dependientes totalmente*

Por último, los medios de pago dependientes totalmente son aquellos que se sirven totalmente de Internet para efectuar sus operaciones.

4.4. Principales medios de pago

Una vez mencionados los aspectos generales de los medios de pago electrónicos estudiaremos los medios más importantes y empleados: la tarjeta electrónica, el dinero electrónico y el pago móvil.

4.4.1. Tarjeta electrónica

■ Introducción

Consideramos necesario delimitar y explicar el sentido de la terminología escogida para el tratamiento de la tarjeta electrónica. Parte de la doctrina alude a la tarjeta de crédito como medio de pago en el comercio electrónico, por ser el término más utilizado para referirse a las tarjetas en general. De la misma manera, se las identifica como tarjetas de pago, tarjetas de plástico, dinero plástico o dinero plastificado. De todas estas denominaciones la más utilizada, tanto por la doctrina como por los usuarios, es la de «tarjetas de crédito». Esta denominación ha sido adoptada debido a la relación subyacente en el contrato de crédito que une al titular de la tarjeta de crédito —en sentido estricto— con la entidad emisora, confundiendo una especie de tarjeta electrónica con el término genérico. En efecto, como veremos más adelante, las tarjetas de crédito son solo una de las modalidades dentro de la amplia gama de tarjetas electrónicas existentes que cumplen funciones diferentes y que en muchos casos ni siquiera otorgan un crédito a su titular. Esto sucede, por ejemplo, con las tarjetas de débito, que permiten la extracción de dinero en cajeros electrónicos, o con los monederos electrónicos.

Hemos optado, por las razones expuestas, por utilizar la expresión «tarjetas electrónicas» —en sentido amplio—, que consideramos el más adecuado a nuestros fines. En efecto, en la actualidad todas las tarjetas cuentan con elementos electrónicos que les permiten funcionar en las redes de pago electrónico.

■ Clasificación

Las tarjetas electrónicas se pueden clasificar de distintas maneras. En este análisis nos referiremos únicamente a las clasificaciones basadas en la tecnología empleada y en la forma de liquidación de las operaciones.

Según la tecnología incorporada a la tarjeta

Utilizamos este criterio para diferenciar las tarjetas que operan en forma manual o en un TPV —es decir, mediante los datos incorporados en la banda magnética— de las que operan con una tecnología más avanzada, algunas de las cuales tienen incorporado un microprocesador que les permite almacenar una gran cantidad de información. En un sentido amplio, hablamos de tarjetas tradicionales y de nuevas tarjetas.

Tarjetas tradicionales

Son las tarjetas electrónicas que contienen los datos impresos o en relieve y que operan mediante banda magnética inserta en el reverso de la tarjeta. Estas tarjetas pueden operar electrónicamente, mediante un TPV o en forma manual, por medio de la impresión mecánica de los datos insertos en relieve, que son fijados en el impreso de nota de cargo por la máquina impresora de tarjeta o «bacaladera». Solo permiten realizar las operaciones tradicionales, esto es, pagos a los proveedores de bienes o servicios adheridos al sistema (y en este sentido, operaciones de pago en el comercio electrónico) y extracción de dinero o consultas en los cajeros automáticos.

Nuevas tarjetas

Identificamos como nuevas tarjetas las que incorporan tecnología y funciones diferentes a las tradicionales, que permiten realizar

compras y operaciones hasta ahora imposibles de ejecutar con la tradicional tarjeta electrónica.

Las nuevas tarjetas permiten, entre otras actividades, realizar operaciones bancarias desde cualquier punto donde se encuentre el titular, cifrar la información, almacenar certificados electrónicos y llevar a cabo operaciones dentro del comercio electrónico. Las nuevas tarjetas han sido objeto de diferentes denominaciones: tarjetas con microchip, con microprocesador o simplemente tarjetas chip, debido al dispositivo incorporado al soporte físico (un microprocesador). Otros las denominan tarjetas inteligentes —*smart cards*— o tarjetas con memoria, por su capacidad de almacenamiento de información.

Las tarjetas inteligentes presentan, frente a las tarjetas con banda magnética, ventajas como fiabilidad, mayor capacidad de almacenamiento de información y una mayor amplitud de usos.

Dentro del comercio electrónico en Internet, ofrecen mayores oportunidades en cuanto a reducción de costes y aumento de la seguridad, sin necesidad de acudir a aplicaciones criptográficas. No obstante, su uso se restringe a los clientes que dispongan de un ordenador personal multimedia con lector de registros.

Dentro de la categoría de las nuevas tarjetas están los monederos electrónicos, las tarjetas de identificación utilizadas en los servicios de banca telefónica o a distancia y las tarjetas electrónicas diseñadas específicamente para el pago en el comercio electrónico.

Monedero electrónico

Se trata de una tarjeta de prepago que permite almacenar unidades monetarias en un microchip con la finalidad de realizar pequeñas compras, en cabinas telefónicas, en taxis, en kioscos, en bares y en pequeños comercios de alimentación en los cuales hasta ahora no se aceptaba la tradicional tarjeta electrónica de crédito y el consumidor debía realizar los pagos en efectivo. El uso del monedero electrónico implica el almacenamiento de una determinada cantidad de dinero a voluntad del titular de la tarjeta. Este dinero se transfiere a la tarjeta desde saldos disponibles a la vista en una cuenta bancaria del usuario del monedero.

Existen principalmente dos modalidades: el monedero electrónico propiamente dicho y el monedero telefónico. Con el monedero electrónico el titular puede adquirir los productos y servicios de los proveedores adheridos al sistema, para lo cual, hasta el momento, es necesario el traslado físico del cliente al establecimiento. Este hecho se debe a que el uso del monedero implica su introducción en el dispositivo adecuado del proveedor de bienes o servicios para registrar la operación realizada y la deducción del saldo del dinero. Para que esto sea posible, los comercios deben contar con los correspondientes terminales lectores del microprocesador, que deben ser facilitados por el emisor.

El importe de las operaciones se registra tanto en el microchip de la tarjeta como en los registros informáticos del banco. El cargo se realiza con el saldo disponible que el titular mantiene en la tarjeta y los importes cargados en el monedero electrónico son adeudados en la cuenta de domiciliación de la tarjeta en el momento en que el titular lo carga en los cajeros automáticos. De este modo, se configura una transferencia electrónica de fondos. La utilización del monedero electrónico implica que el titular debe asumir los riesgos en caso de utilización fraudulenta o irregular o en caso de pérdida, incluso después de haberla notificado al banco.

El monedero telefónico no hace necesario el traslado del usuario al establecimiento del comercio, ya que la orden de compra y de pago se realiza desde su teléfono móvil.

Tarjeta de identificación en los servicios de telebanco

El servicio de telebanco, banca electrónica o a distancia, permite a los clientes realizar las operaciones tradicionales bancarias sin estar físicamente en una sede del banco. Para lograrlo se requiere la existencia de una tarjeta electrónica que se emite con la finalidad de facilitar, mediante el uso de teléfonos o de ordenadores personales, la ejecución de determinadas operaciones. Mediante una simple llamada telefónica o la conexión a una red, que puede ser Internet u otra red convenida por las partes, el cliente, con el número asignado en la tarjeta, el PIN (*personal identification number*, número

personal de identificación), que es su clave secreta, y con las correspondientes claves de acceso puede solicitar información sobre su estado de cuenta o sobre las operaciones del banco, además de ordenar transferencias, comprar y vender valores, pedir suscripciones y reembolsos de fondos, solicitar talonarios, dar orden sobre tarjetas electrónicas, cambiar su información personal y realizar todas las operaciones convenidas previamente con el banco emisor.

Tarjetas para el pago en el comercio electrónico

Las tarjetas tradicionales pueden operar en el comercio electrónico. En este caso, el titular envía sus datos y los de la tarjeta al proveedor aceptante, quien a su vez los remite a la entidad emisora para que gestione y autorice el pago. Su inviolabilidad se basa en el uso de la clave secreta (PIN) por parte del titular y en las claves internas de la entidad.

El problema del uso de las tarjetas electrónicas tradicionales en estos casos es la facilidad de vulneración de los datos de la tarjeta. En efecto, pueden ser interceptados por cualquier persona que tenga acceso a la red. Esta posibilidad produce inseguridad entre los contratantes sobre la autenticidad del mensaje, facilitando la práctica de operaciones fraudulentas.

Por estas razones, el pago de las operaciones concertadas en el comercio electrónico en redes abiertas como Internet precisa de mayores medios de seguridad. Este resguardo se consigue con el uso de la firma digital, de tarjetas electrónicas inteligentes diseñadas especialmente para el comercio electrónico, basadas en *criptosistemas* de claves asimétricas, y con el establecimiento de protocolos comunes que amplían y modifican el sistema de registro de datos.

Según la forma de liquidación de las disposiciones realizadas

Atendiendo al plazo que media entre el momento de la transacción y el momento en que se carga el importe de la operación en la cuenta del titular, las tarjetas electrónicas pueden ser de crédito, de débito, prepagadas y de cargo diferido.

Las tarjetas de crédito

Son denominadas en doctrina «tarjetas de crédito en sentido restringido», pues funcionan mediante una línea de crédito que concede el banco a sus clientes, documentada en el contrato de emisión, en virtud del cual el titular de la tarjeta electrónica de crédito puede disponer de bienes y servicios sin que se produzca un cargo inmediato en su cuenta. Se pueden establecer diferentes formas de liquidación del crédito, ya sea obligando a pagar mensualmente la totalidad del saldo o mediante pagos parciales, que pueden ser fijos o variables, con el correspondiente cargo de intereses.

Las tarjetas de débito

Están vinculadas a una cuenta corriente o de depósito que opera exclusivamente de forma electrónica y automática. Las operaciones realizadas por el cliente son adeudadas inmediatamente si el terminal o el cajero están conectados al ordenador central (operación *on line*) o unos momentos después, si no están conectados (operación *off line*). Las operaciones de compra realizadas mediante tarjetas de débito configuran una típica transferencia electrónica de fondos, trasladando el dinero de la cuenta del titular a la cuenta del proveedor que acepta la tarjeta (que necesariamente debe estar conectado a un TPV) o descargándolo del saldo del cliente cuando ha realizado una disposición de efectivo en un cajero automático. Estas tarjetas no conceden crédito en ningún caso, aun cuando las operaciones no sean cargadas de forma inmediata en la cuenta de titular. En el caso de operaciones *off line*, no se considera que el banco haya concedido crédito al cliente, ya que para hacerlas es imprescindible que el cliente tenga fondos suficientes en su cuenta, obligándose contractualmente a no efectuar disposiciones que no estén cubiertas por el saldo disponible. La tarjeta de débito desempeña un papel equivalente al del dinero en efectivo. La banda magnética incorporada a los sistemas de tarjetas permite que el abono al comerciante y el cargo en la cuenta del usuario se hagan en forma instantánea y simultánea (en el caso de las operaciones *on line*).

Las tarjetas de cargo diferido

Al igual que las tarjetas de crédito en sentido restringido, conceden crédito a su titular pero se diferencian de aquellas en la forma de liquidar el crédito y en el límite establecido. Estas tarjetas no establecen un límite de gastos. Operan mediante la acumulación de los pagos realizados para su cargo diferido al final del mes. El titular tiene la obligación de abonar mensualmente la totalidad de las operaciones realizadas. El crédito con cargo de intereses es opcional para la institución financiera, que puede otorgarlo a solicitud del cliente. En este caso, la tarjeta de cargo diferido opera en sentido similar a la tarjeta de crédito, en la que el titular puede realizar pagos fraccionados con el correspondiente abono de intereses. El ejemplo típico de estas tarjetas lo tenemos en las del Diners Club y en las de American Express.

Las tarjetas prepagadas

A diferencia de las tarjetas de crédito, de débito y de cargo diferido, el cargo en la cuenta asociada a la tarjeta del titular es previo a la operación de disposición del dinero. El titular, de acuerdo con sus necesidades, decide el importe a cargar en ellas antes de que se lleve a cabo la operación (la compra en un establecimiento mercantil o su uso en una cabina telefónica). Dentro de esta categoría están las tarjetas diseñadas específicamente para pagos en Internet, que funcionan mediante el cargo previo del dinero en el correspondiente soporte electrónico.[73]

- **Sujetos participantes y relaciones contractuales en el empleo de la tarjeta electrónica**

Los sujetos participantes en una operación de pago realizada en el comercio electrónico mediante una tarjeta electrónica son el emisor de la tarjeta, el titular de la tarjeta, los intermediarios electrónicos (el proveedor aceptante, el servidor del emisor, el servidor del

[73] Un ejemplo de este tipo de tarjetas es la tarjeta VÍABCP, emitida por el Banco de Crédito del Perú.

titular y el servidor del proveedor aceptante) y el prestador de servicios de certificación. Además, participa la empresa propietaria de la marca que autoriza la emisión de la tarjeta en régimen de franquicia o en licencia de uso, según el caso.

El emisor

Es una entidad de crédito, en el caso de las tarjetas bancarias, mientras que en el caso de las tarjetas no bancarias es un proveedor de bienes o servicios o un establecimiento financiero de crédito (una sociedad especializada en la emisión de tarjetas, por ejemplo).

Según los casos, es el sujeto que emite la tarjeta con la autorización de la empresa propietaria de la marca de la tarjeta. El emisor se vincula con la empresa propietaria de la marca generalmente por un contrato de franquicia que posibilita el uso internacional de la tarjeta. El emisor se vincula con el titular, en cambio, mediante un contrato de emisión de tarjeta, que puede asumir distintas modalidades según el tipo de tarjeta (de crédito, de débito, de cargo diferido o prepago). El contrato le permite al usuario utilizarla según las condiciones pactadas.

El titular

Es la persona física que tiene el derecho a usar la tarjeta legítimamente. Es el cliente de la entidad de crédito o del proveedor de bienes o servicios que emite la tarjeta y que se obliga frente a ellos a cumplir con las condiciones generales establecidas en el contrato de emisión. Al mismo tiempo es el consumidor que adquiere los bienes o servicios que le suministra el proveedor afiliado al sistema de tarjetas.

Como podemos observar, el contratante puede ser una persona jurídica, pero solo pueden ser titulares de las tarjetas las personas físicas, pues la tarjeta electrónica es un documento nominativo, personal e intransferible.

Los proveedores de bienes o servicios aceptantes de la tarjeta

El proveedor de los bienes o servicios aceptante es cualquier persona, natural o jurídica, que dentro de su actividad comercial o

profesional acepta el pago con tarjeta en virtud de una relación contractual con la entidad emisora. Mediante esta relación contractual se obliga previamente a aceptar la tarjeta, a fin de que los clientes de la tarjeta puedan beneficiarse de las ventajas de utilizar este medio de pago.

El contrato que une al emisor con el proveedor aceptante se denomina «contrato de admisión o de aceptación de la tarjeta» y contiene una serie de condiciones a las que se adhiere el proveedor de bienes o servicios. En virtud del contrato de admisión, el proveedor aceptante se compromete a admitir la tarjeta como medio de pago en sus transacciones comerciales, con la obligación de adecuar sus equipos a las características de funcionamiento y de transmisión de la información utilizadas en el sistema. Por su parte, el emisor se obliga frente al proveedor a descontar las facturas y a hacerlas efectivas, deduciendo la comisión correspondiente.

El establecimiento comercial, al ser el lugar donde se realiza la operación, en el caso del comercio electrónico, adquiere la condición de establecimiento virtual al ofrecer sus servicios en Internet valiéndose de una página web de fácil acceso al cliente. Esta página contiene información detallada del proveedor de bienes o servicios, de sus productos, de sus precios, de los servicios y de cualquier otra información que el cliente requiera para realizar una transacción en la modalidad de comercio electrónico.

Los intermediarios electrónicos

En las operaciones de comercio electrónico realizadas en Internet intervienen, además de los sujetos indicados, los intermediarios electrónicos que facilitan la conexión y el acceso a la red. Los intermediarios proporcionan servicios adicionales, haciendo operar la infraestructura de las telecomunicaciones sobre las que se realizan las transacciones. De este modo, mantienen sus convenios privados con el emisor, con el titular y con el proveedor de bienes o servicios adherido al sistema de tarjetas.

De estos sujetos, nos interesa el caso del proveedor de acceso y el del centro servidor, que en ocasiones puede tratarse de la misma

persona, por lo que pueden originarse distintos casos de responsabilidad. En este caso, nos centraremos en el estudio de la posición jurídica del servidor que al mismo tiempo comercializa la información y proporciona acceso a Internet.

El pago mediante tarjeta en una operación comercial electrónica involucra principalmente al servidor del proveedor de bienes o servicios, al servidor del titular y al servidor del emisor, asumiendo que es el emisor quien autoriza el pago mediante tarjeta.

En el caso del servidor del proveedor de bienes o servicios, le presta el servicio para gestionar su nombre de dominio en Internet. Así, el proveedor de bienes o servicios estará representado, generalmente, con su propio nombre o marca mediante la publicación de la página web en Internet. De este modo, cualquier persona, desde cualquier parte del mundo, puede consultar la información de la entidad y de sus productos.

El particular —en nuestro caso el titular de la tarjeta— generalmente contrata con un proveedor de acceso (aunque también lo puede hacer directamente con el servidor) la conexión a Internet. El proveedor de acceso le asignará sus claves de identificación (*login* y *password*). El acceso al servicio se realizará mediante el código del cliente y el *password*, que son claves personales e intransferibles generadas por la empresa que da acceso a Internet. Se entiende que el cliente asume los riesgos por el quebrantamiento de la confidencialidad y por el mal uso de las claves y códigos de acceso. La pérdida de la información por culpa o por negligencia del proveedor de acceso o del servidor, según los casos, será su responsabilidad. En este sentido, deberá responder no solo ante el cliente sino, también, ante terceros, de los daños y perjuicios que se deriven de la manipulación incorrecta o no autorizada que provoque averías o deterioros en el servicio o la pérdida o destrucción de la información.

El servidor del emisor juega un papel importante, pues es el emisor quien finalmente emite la autorización para que el proveedor de bienes y servicios acepte la tarjeta como medio de pago.

Los servidores son terceros ajenos a las relaciones contractuales propias del contrato de tarjeta. En este sentido, es importante

analizar su actuación, para determinar su responsabilidad por la alteración o pérdida del mensaje durante su transmisión. Se entiende que tienen la obligación de protegerse frente a intrusiones e intentos de acceso no autorizados que puedan llegar a un uso fraudulento de la información transmitida.

El prestador de servicios de certificación

En las operaciones realizadas con tarjetas en el comercio electrónico se adiciona el prestador de servicios de certificación como tercera parte de confianza entre comprador y vendedor, para garantizar la emisión, recepción y contenido del mensaje, así como la identidad de las partes. Se trata de un tercero que actúa como intermediario en la comunicación certificando claves; validando fecha, hora y lugar; y cifrando el documento electrónico con sus claves privadas para luego enviarlo a las partes que lo descifrarán con la clave pública, posibilitando la prueba de la notificación, autoría, no repudio, autenticación, integridad, etc.

Si bien es cierto que hemos analizado con profundidad a los prestadores de servicios de certificación, consideramos necesario referirnos específicamente a ellos en lo concerniente a su participación en el empleo de las tarjetas electrónicas.

En el caso de los pagos realizados con tarjetas electrónicas, el prestador de servicios de certificación mantiene una relación contractual principalmente con el emisor, que es la parte verificadora del sistema que autoriza el pago con tarjeta. Este hecho no impide que el titular de la tarjeta pueda acceder también a los servicios que presta esta entidad, solicitando su par de claves para asegurar su intervención en el comercio electrónico, mediante el cifrado de su mensaje. El titular puede contratar directamente con el prestador de servicios de certificación o por medio de la entidad o establecimiento financiero de crédito emisor, que puede ofrecer el financiamiento dentro de sus servicios.

El prestador de servicios de certificación se involucra, primero, con los emisores; segundo, con el suscriptor; y, finalmente, con el tercero usuario. El suscriptor es la persona física o jurídica titular

del certificado emitido por el prestador de servicios de certificación, cuyo nombre aparece incluido en el documento. Posee legítimamente una clave privada que se corresponde con la clave pública contenida en el certificado. El tercero usuario es cualquier persona que confía en la firma digital creada por el suscriptor mencionado en el certificado y puede usar la clave pública incluida en el certificado para verificar que la firma digital fue creada con la correspondiente clave privada.

En las operaciones realizadas con tarjetas electrónicas, el suscriptor puede ser el proveedor aceptante o el titular. Estos, a su vez, pueden actuar también como terceros usuarios, en tanto que los emisores de la tarjeta y las empresas propietarias de la marca, además de los suscriptores, pueden actuar, y de hecho actúan, como prestadores de servicios de certificación. Es el caso de Visa y de Master Card. De esta manera, los titulares y los aceptantes de las tarjetas pueden contratar con los emisores en su función de prestadores de servicios de certificación, independientemente de su desempeño como emisores de la tarjeta o propietarios de la marca de tarjeta.

- **Validez del cumplimiento de la obligación de pago mediante una tarjeta electrónica**

Para la validez del cumplimiento de la obligación de pago en el comercio electrónico mediante tarjetas es necesario, en primer lugar, que las partes admitan las tarjetas como medios de pago. Esta condición se debe a la libertad de las partes de pactar la forma en la que se realizará el pago de las obligaciones contraídas y a la imposibilidad de obligar al acreedor a aceptar el pago de una forma no pactada o aceptada por él mismo.

En una operación de compraventa electrónica simple (sin la intervención del prestador de servicios de certificación), el mecanismo de pago mediante tarjetas opera mediante la inserción de los datos personales del cliente y los de su tarjeta en un formulario de pedido, que es enviado por el cliente al proveedor de bienes o servicios vía *e-mail* o mediante la web. El proveedor, utilizando este

mismo proceso, los remite al banco emisor para la autorización y la gestión del pago.

En el sistema electrónico de pagos en el que interviene el prestador de servicios de certificación se suceden las siguientes etapas:

- El comprador inicia la transacción identificándose ante el comerciante mediante el uso de la firma digital.
- El comprador recibe la firma digital del comercio e identifica al vendedor.
- El comprador envía un formulario de pedido cifrado y firmado en el cual el comerciante solo puede leer la solicitud y no los datos de la tarjeta.
- El comerciante identifica al cliente mediante el certificado digital.
- El banco recibe las autorizaciones de pago del cliente por medio del comerciante o directamente del cliente, mediante el uso de la firma digital dual, y consulta al emisor de la tarjeta en caso de no ser él mismo, para obtener la autorización firmada de la transacción. En este caso, el cliente ejecuta una función con su clave pública y con la privada, y comprime el mensaje transformándolo en un texto ilegible. Al llegar al proveedor este lo descifra sin poder acceder a los números de la tarjeta. De esta manera se consigue la seguridad en la transacción.

- **Efectos del cumplimiento de la obligación del pago mediante una tarjeta electrónica**

Para determinar los efectos del pago realizado mediante una tarjeta electrónica, es necesario hacer una distinción según el tipo de tarjeta utilizada. Esta diferenciación es importante, pues, como veremos, los efectos del pago difieren según el tipo de tarjeta electrónica.

El pago realizado con tarjeta electrónica de crédito

Produce principalmente efectos liberatorios para el titular de la tarjeta. No así para el emisor, quien por virtud del contrato de emisión se obliga a garantizar el pago de las obligaciones contraídas mediante tarjetas por el titular. De esta manera, el titular queda liberado de la deuda, pero la obligación no se extingue hasta que el

emisor no satisfaga al proveedor aceptante con el importe de la deuda.

El pago realizado con tarjeta electrónica de débito

Se producen todos los efectos del pago que hemos indicado. El titular se libera de la obligación extinguiéndola y satisfaciendo al acreedor, quien recibe en su cuenta, por vía electrónica, el importe de la deuda. El pago se hace con los fondos que el titular tenga disponibles en la cuenta bancaria asociada a la tarjeta. Se trata, en este sentido, de una operación similar al pago en dinero efectivo, ya que opera automáticamente mediante el sistema de transferencias electrónicas de fondos: si el titular carece de fondos, el proveedor debe rechazar el pago. Si el emisor da la autorización erróneamente o concede un descubierto en la cuenta (es decir, la posibilidad de acceder a la información de la cuenta), la orden se considera irrevocable. En este caso se producen los efectos indicados en el caso de las tarjetas electrónicas de crédito: el emisor se obliga frente al proveedor y le asiste el derecho de repetición contra el titular. Esta circunstancia excepcional en ningún momento desnaturaliza el uso de la tarjeta de débito para configurarla como una tarjeta de crédito.

El pago realizado con «tarjetas virtuales», específicas para pagos en Internet

Al tratarse de una tarjeta prepagada, el pago produce los mismos efectos del pago efectuado en dinero efectivo. En otras palabras, se satisfacen los intereses del acreedor, la deuda se extingue y el deudor se libera de su obligación. Estas tarjetas funcionan en una forma similar a las tarjetas de débito, pues los fondos se transfieren automáticamente de una cuenta a otra.

La diferencia fundamental radica en que las tarjetas de débito están asociadas a una cuenta en la que se encuentran los fondos del titular, mientras que los fondos disponibles de las tarjetas prepagadas se transfieren previamente a la tarjeta, independientemente de la existencia de una cuenta asociada. Por este motivo, no se necesita la comprobación de fondos en la cuenta ni la autorización de la

entidad emisora, ya que el dinero está contenido en el propio soporte electrónico.

- **Prueba de pago con la tarjeta electrónica**

En una operación tradicional de pago con una tarjeta electrónica tradicional, la firma sobre el papel que se genera con el TPV o el impreso con copia al carbón de la bacaladera. Se identifica con el recibo de pago emitido por el acreedor, que es la prueba del pago para los sujetos participantes (para el cliente, para el proveedor de bienes o servicios y para el emisor de la tarjeta).

En el caso de una operación de compra realizada mediante ordenadores interconectados, es decir, por Internet, sin la presencia física de las partes y con la ausencia de un recibo en papel, se presenta el problema relacionado a la prueba de pago. No obstante, el pago por dispositivos electrónicos puede ser acreditado mediante la certificación del asiento en cuenta corriente bancaria, por medio de la aceptación por el comprador, por la intervención de un prestador de servicios de certificación o con la ejecución de la función de intermediación a la que nos referiremos en el siguiente capítulo (véase la página 230).[74] En este sentido, los pagos realizados mediante apuntes electrónicos en cuenta por medio de sistemas de pago electrónico en redes de comunicación, no difiere en esencia del pago realizado con una tarjeta electrónica.

En las compras realizadas en una operación de comercio electrónico simple, la prueba la constituyen los formularios de pedidos enviados por el cliente en los que consta el número de unidades solicitadas, su identificación, los datos de la tarjeta, el precio, los gastos de envío y los datos requeridos para la entrega: dirección postal y teléfono de contacto.

Otra forma de comprobar el pago es con la factura electrónica. En un contrato de compraventa, la factura cumple la función de reflejar las circunstancias que conciernen a la fase ejecutiva del

[74] Con el empleo de un certificado digital transaccional.

contrato, como son la constatación del estado de las mercancías, la fecha, la hora y el lugar de entrega y la constancia de que se ha pagado el precio. En este sentido, la factura sirve para comprobar tanto las obligaciones del vendedor como las del comprador.

En el pago mediante tarjetas electrónicas, en una operación tradicional, la factura es la nota de cargo que el titular firma como comprobante de que se ha entregado las mercancías y se ha pagado el precio. En una operación de comercio electrónico, este sistema de facturación no existe, pero podríamos llegar a él con el empleo de la facturación electrónica.

En nuestro ordenamiento jurídico aún no se ha regulado la emisión de facturas electrónicas. Sin embargo, podríamos recurrir a las disposiciones de la Convención de Viena sobre Compraventa Internacional de Mercaderías, para emplear estos documentos como medios de prueba de pago.

El artículo 11 de la Convención de Viena sobre Compraventa Internacional de Mercaderías no se opone a la admisión de registros computarizados como elementos probatorios. Por lo tanto, al amparo de este cuerpo legal, que está incorporado en nuestro ordenamiento jurídico, es posible el empleo de la factura electrónica en las compraventas electrónicas internacionales.

Por último, la factura electrónica, contenida en un soporte informático, sustituye a la factura en papel y tiene los mismos efectos que se atribuyen a esta última. Esta característica no es más que otra expresión del principio de equivalencia funcional entre el documento electrónico y el documento en papel, enunciado en el artículo 5 de la Ley Modelo de UNCITRAL sobre comercio electrónico, que dispone que: «No se negarán efectos jurídicos, validez o fuerza probatoria a la información, por la sola razón de que esté contenida en forma de mensaje de datos». Para que la factura electrónica sea válida, la información contenida en la factura emitida y recibida debe ser idéntica. Este requerimiento se puede comprobar mediante el cifrado asimétrico del mensaje de datos que contiene la factura.

- **Seguridad**

Como hemos indicado, uno de los mayores problemas que se presentan en las transacciones verificadas en el comercio electrónico que se llevan a cabo en entornos abiertos como Internet se refiere a la seguridad en el pago ante la posibilidad de vulneración del mensaje y la alteración de datos de trascendental importancia. Ante esta situación, se hace necesario implementar mecanismos de seguridad específicos para el pago. Actualmente, encontramos estos mecanismos de seguridad en los sistemas criptográficos de la firma digital; en la emisión de certificados por parte de los prestadores de servicios de certificación, que ya hemos explicado; y en los protocolos de seguridad desarrollados principalmente por las empresas propietarias de las marcas de tarjetas electrónicas, que serán estudiados a continuación.

Las entidades emisoras y propietarias de tarjetas electrónicas, y las diferentes empresas de informática han trabajado en conjunto en la especificación de protocolos de seguridad para garantizar los datos transmitidos en redes abiertas mediante el sistema de encriptación. Los principales protocolos de seguridad elaborados son el SSL (*Secure Sockets Layer*) y el SET (*Secure Electronic Transactions*). Este último es el más difundido y utilizado en las operaciones de comercio electrónico.

Protocolo SET

El Protocolo SET fue desarrollado por Visa y por Master Card Internacional junto con las empresas informáticas. Garantiza la confidencialidad de la información tanto económica como la relacionada a los bienes comprados (permite cifrar separadamente la información). De este modo, ofrece servicios de autenticación (pues todas las partes pueden autenticarse mutuamente mediante certificados electrónicos), de confidencialidad (ya que la información sobre los datos de compra y sobre la tarjeta se transmiten cifrados), de integridad (pues se garantiza la inalterabilidad del mensaje) y de gestión de pagos (autorizaciones y liquidaciones de pagos). El uso de formatos de mensajes y protocolos específicos garantiza su interoperabilidad.

Para lograr estos objetivos utiliza la encriptación de mensajes, firmas y certificados electrónicos. El protocolo SET, como sistema híbrido que incorpora los dos sistemas de encriptación (simétrico y asimétrico), permite aprovechar la rapidez del sistema simétrico, evitando la lentitud de los sistemas asimétricos.

Sujetos participantes en una operación de comercio electrónico mediante el uso del protocolo SET

A diferencia de lo que ocurre con el protocolo SSL, el SET involucra a todas las partes participantes en una operación de *e-commerce*. Para que todos los sujetos intervengan en una operación de esta naturaleza, es necesario que cada uno tenga una firma digital. Los sujetos son los siguientes:

- El titular de la tarjeta
- El vendedor o proveedor de servicios o productos
- El banco emisor de la tarjeta
- El banco adquirente, que procesa las transacciones con tarjeta y autoriza el pago mediante el sistema de pasarela de pagos
- El prestador de servicios de certificación que certifica las claves públicas del titular de la tarjeta, del aceptante y de los bancos.

Requisitos para comprar con el protocolo SET

• *Software* SET. Comúnmente denominado «*software* de gestión de tarjeta», o «*wallet*». En él, el cliente almacenará información sensible, como el banco emisor del certificado SET o su número de cuenta, que es suministrado por la entidad emisora de la tarjeta o por el proveedor de bienes o servicios.

• Certificado digital SET. El certificado digital SET es emitido por la misma entidad emisora de la tarjeta y asegura la legitimidad en su uso. Si se tiene más de una tarjeta electrónica, se requiere un certificado distinto para cada una. Del mismo modo, el proveedor de bienes o servicios necesitará un certificado digital diferente para cada marca de tarjeta que quiera aceptar. El uso de estos certificados proporciona al comprador la misma seguridad que cuando paga con tarjeta en el establecimiento físico. Los pagos mediante

SET solo se podrán efectuar en los establecimientos virtuales que ofrezcan seguridad SET mediante la exhibición del logotipo en su página web.

• Monedero digital.[75]

Proceso de ejecución del protocolo SET en una compra

La seguridad en la transacción de pago con tarjetas mediante el uso del protocolo SET se basa en el sistema de firma doble. Nos valdremos del cuadro de la página anterior para explicar el funcionamiento de este protocolo al realizar un pago.

A continuación describiremos en detalle el cuadro para determinar la secuencia para la realización del pago empleando el protocolo SET.

1. En la primera fase de la ejecución, el *cliente*, que es la persona que celebra un contrato con el proveedor de servicios o bienes (a quien en el gráfico se denomina *comercio*), le remite un mensaje que contiene dos aspectos básicos: la información relativa al pedido (relacionada con las características de los bienes o servicios a contratar), que es cifrada con la clave pública del comercio, obteniéndose la información del pedido cifrado (IPC); y la información relativa al pago, que es cifrada con la clave pública del banco emisor, con lo que se obtiene la información del pago cifrado (IpgC). Las dos informaciones cifradas integran la hoja de pedido.

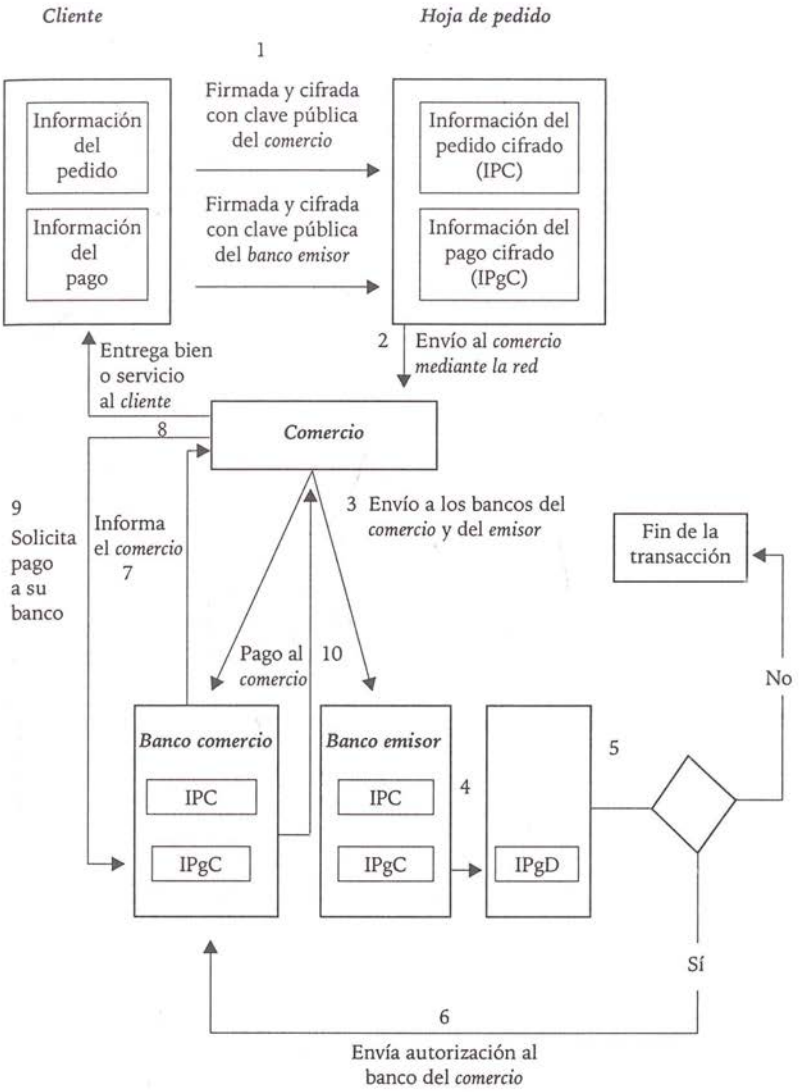
La ventaja de la encriptación del mensaje mediante dos claves públicas radica en que el *comercio* no podrá conocer la información relativa al pago. El *banco* tampoco tendrá acceso a la información relativa al pedido, pues ninguna de estas entidades tiene la clave privada de la otra, que le permitiría descifrar la información cifrada con su clave pública.

2. En la segunda fase, el *cliente* envía al *comercio* la hoja de pedido (que contiene la IPC y la IpgC).

---

[75] El monedero digital es otra de las denominaciones del monedero electrónico.

Ejecución de protocolo SET en una compra



1 Descifra con su clave privada.

2 Verifica fondos del cliente y autoriza.

3. Una vez que el *comercio* haya recibido la hoja de pedido, comprueba su veracidad y la retransmite tanto a su *banco* como al banco emisor del medio de pago electrónico (tarjeta electrónica o dinero electrónico), denominado *banco emisor* en el gráfico.

4. Luego, el *banco emisor* recibe la hoja de pedido y descifra la información del pago cifrado (IpgC), obteniendo la información del pago descifrada (IpgD). No puede, como hemos indicado, conocer la información relativa al pedido, ya que solo puede ser descifrada con la clave privada del *comercio*.

5. Obtenida la IpgD, el *banco emisor* procede a verificar la disponibilidad de fondos del *cliente*. En caso de que los fondos sean suficientes para pagar la compra de los bienes o servicios, autoriza el pago. Si no dispone de fondos, la operación de pago concluirá.

6. Una vez autorizada la transacción, el *banco emisor* lo comunica al *banco del comercio*.

7. Cuando se haya obtenido la autorización de la operación, el *banco del comercio* le envía un mensaje firmado y cifrado digitalmente, informando a su cliente que la operación ha sido autorizada y adjuntándole un testigo de transferencia de fondos. El comerciante almacena en su TPV estos dos elementos. En este momento, el comerciante sabe que la operación es viable y que el pago está asegurado.

8. Una vez recibida la autorización de la transacción, el *comercio* cumple con ejecutar la entrega de los bienes o servicios contratados por el *cliente*.

9. Luego, el *comercio* solicita a su *banco* el pago del importe correspondiente a los servicios o bienes contratados.

10. Finalmente, el *banco* del *comercio* abona en su cuenta el importe solicitado.

Dificultades en el empleo del protocolo SET

A pesar de la seguridad que aporta el uso del protocolo SET, su implantación ha sido criticada debido a que se trata de un proceso complejo y lento, al requerir sistemas asimétricos de cifrado y la comprobación de los distintos certificados de las partes. En efecto,

en cada comunicación el receptor debe comprobar el origen de la transmisión por medio del sistema de jerarquías de certificados de los distintos proveedores que los hayan emitido. De otro lado, los clientes deben darse previamente de alta en el sistema, solicitando la instalación del *wallet* (*software* SET) y la conexión con el proveedor de servicios de certificación para la correspondiente emisión de las claves, operación que toma una o dos semanas.

Protocolo SSL

Para explicar el funcionamiento de este protocolo nos valdremos del aporte de Ortega Díaz.[76]

En 1994, junto al lanzamiento de la primera versión de su navegador, la empresa norteamericana Netscape Communications Corporation propuso el protocolo de pago más extendido en la red. En la actualidad, este protocolo es admitido por las dos grandes compañías que se reparten el mercado de los navegadores, Netscape y Microsoft.

Mediante este protocolo de fácil empleo (para usarlo basta con abrir una página web cuya dirección comience con las siglas http://), el usuario puede realizar una operación de pago con solo rellenar un formulario con sus datos personales y bancarios. Mediante un canal seguro los datos son cifrados con criptografía simétrica y enviados al comerciante, quien los recibirá, los descifrará y ejecutará el pago en la entidad bancaria correspondiente.

No obstante, a pesar de su implantación y de la facilidad de su uso, el SSL presenta un gran inconveniente: no es seguro o, al menos, no tiene una seguridad óptima. Así, el SSL ofrece funciones de integridad y de confidencialidad en las comunicaciones realizadas entre el consumidor y la página web del comerciante alojada en el servidor, dejando al margen al emisor de la tarjeta, que es una de las tres partes implicadas en una operación de pago con tarjeta. De esta forma, nos señala la profesora Martínez Nadal, «[l]os comerciantes

---

[76] ORTEGA DÍAZ, Juan Francisco. «El cumplimiento del pago por medios electrónicos». En <www.vlex.com/redi/No._36_-_Julio_del_2001/9>.

corren riesgo de utilizaciones fraudulentas de las tarjetas, e igualmente el comprador no queda protegido del riesgo de que un comerciante deshonesto utilice ilícitamente su tarjeta».

4.5. Dinero electrónico

4.5.1. Definición de dinero electrónico

Antes de señalar algunas definiciones de dinero electrónico, nos parece importante definir el dinero en términos generales. Según el Diccionario de la Real Academia Española (DRAE), el dinero es un «[m]edio de cambio de curso legal».[77]

De acuerdo con esta definición, el dinero es un bien que representa un determinado valor patrimonial. Esta característica le permite servir como medio de cambio de bienes. Se desprende de la misma definición que el dinero debe estar dotado de un reconocimiento o respaldo legal.

Como vemos, el dinero es el bien que por excelencia puede ser empleado para el pago de obligaciones. Nótese que la definición citada no hace alusión alguna al soporte físico del dinero, por lo cual se podría decir válidamente que esta definición de dinero abarcaría al dinero electrónico, si no fuera por la mención a su reconocimiento legal.

Una vez citada la definición genérica de dinero pasaremos a comentar algunas definiciones de dinero electrónico. De acuerdo con Juan Ortega,

> 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.[78]

---

[77] *Diccionario de la Real Academia Española*. Vigésima segunda edición. Tomo IV, p. 558.

[78] ORTEGA DÍAZ. Ob. cit.

Frente a la definición del DRAE, la de Juan Ortega es más específica, ya que se refiere a la representación de un valor abstracto respaldado por una autoridad legal, como característica genérica, y al medio en el que se encuentra representado (es decir, su representación electrónica) como característica diferenciadora.

Según Gerardo Vilet, el dinero electrónico «[e]s básicamente la representación por medios electrónicos de la capacidad de realizar transacciones financieras sin tener que mediar, para ello algún intercambio físico de monedas o papeles».[79]

En esta definición se ha obviado el respaldo legal que tiene el dinero en términos generales. A nuestro parecer, al ser el dinero un bien que representa un valor abstracto —lo que le permite ser el medio por excelencia ideal para el pago de obligaciones— se le debe atribuir este valor abstracto con el respaldo legal de una autoridad pública. Solo así podrá ser un medio oponible y eficaz para extinguir obligaciones *erga omnes*.

De acuerdo con los comentarios a las definiciones citadas, proponemos la siguiente definición: el dinero electrónico, también llamado *e-money* o *cibermoneda*, es la representación de un valor abstracto por medios electrónicos, respaldado por una autoridad pública, que permite la realización de todo tipo de transacciones patrimoniales.

Al respecto hay ciertos puntos que debemos mencionar. En primer lugar, la participación de una autoridad pública en la creación del dinero electrónico no debe ser directa sino indirecta. En otras palabras; la autoridad pública no debe atribuir directamente el valor económico al dinero electrónico. Deberá participar autorizando, fiscalizando y supervisando las empresas que otorguen el valor económico al dinero electrónico directamente. Será el mercado el que determine cuáles empresas financieras prestarán más satisfactoriamente los servicios de emisión del *e-money*. Esta precisión responde al hecho de que los conceptos de «mercado» y «eficiencia»

---

[79] VILET ESPINOSA, Gerardo Javier. «El dinero electrónico en México». En <http:// edipo.madm.uaslp.mx/El%20dinero%20electr%C3%B3nico.htm>.

reemplazan ciertas funciones del Estado, como sucede con las entidades de certificación.

En segundo lugar, esta definición está acorde con el principio de equivalencia funcional, al comprender todo tipo de soporte electrónico que pueda representar este valor abstracto. Por último, se trata de una definición amplia respecto del uso que se pueda dar al dinero electrónico. Por este motivo, señalamos que permite la realización de todo tipo de transacciones patrimoniales (es decir, transacciones en las que exista desplazamiento patrimonial).

4.5.2. Sujetos participantes en el empleo del dinero electrónico

Los sujetos participantes en el uso del dinero electrónico son los siguientes:

- El banco emisor, que suministra el *software* necesario para la creación del dinero y se atribuye valor patrimonial
- El titular del dinero electrónico
- El proveedor de servicios o bienes, a quien denominaremos el *comercio*

4.5.3. Creación del dinero electrónico

En el gráfico de la página siguiente, elaborado en base a la explicación de Juan Francisco Ortega Díaz,[80] mostramos el proceso de creación del dinero electrónico.

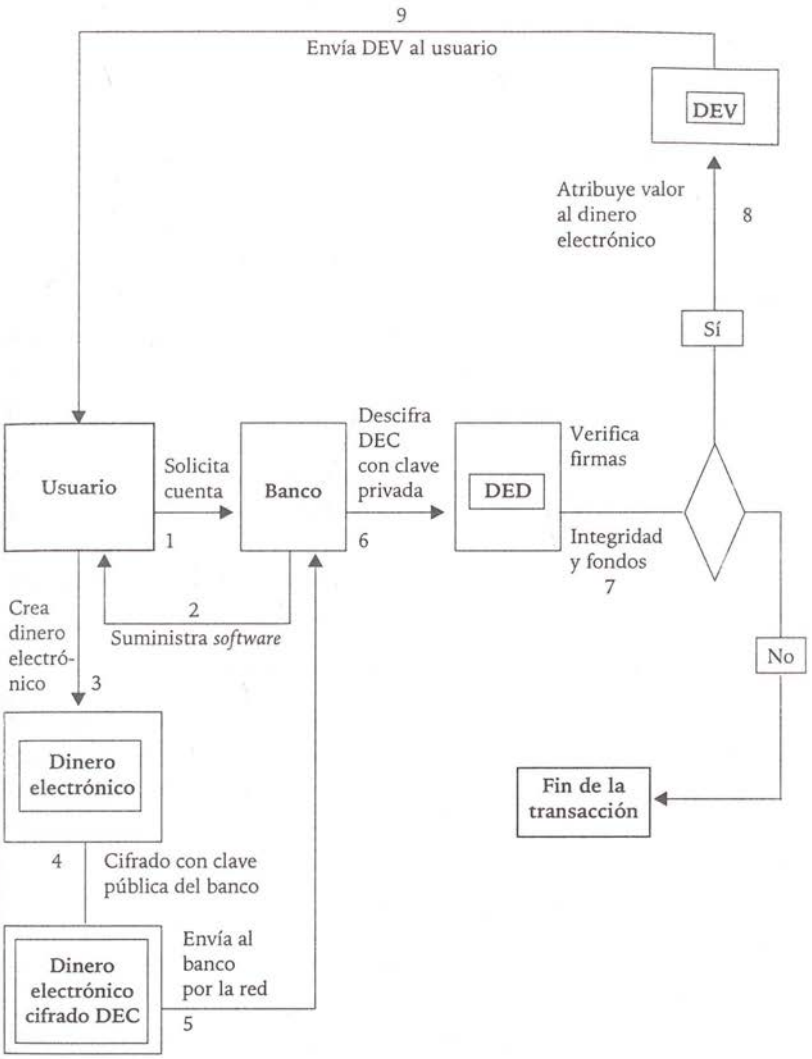
1. El usuario debe convertirse en titular de una cuenta corriente en una entidad bancaria que emita moneda electrónica. Para esto deberá firmar el contrato de cuenta corriente correspondiente. Este contrato deberá incluir la posibilidad de la emisión de dinero electrónico.

2. Una vez suscrito el contrato de cuenta corriente, y siempre que el cliente lo solicite, el banco le suministrará el *software* para la creación de dinero electrónico. Con este *software*, el cliente podrá «crear» tanto e-*money* como dinero tenga en su cuenta real.

---

[80] ORTEGA DÍAZ. Ob. cit.

Creación de dinero electrónico



3. En la tercera etapa el cliente, empleando el *software* gestor de la cuenta del usuario, crea dinero electrónico, atribuyendo a cada *cibermoneda* un número de serie aleatorio.

4. Una vez creada la *cibermoneda* con el número de serie aleatorio, el usuario la firma digitalmente con la clave pública del banco, obteniendo el dinero electrónico cifrado (DEC).

5. El DEC es enviado al banco por la red.

6. Cuando el banco recibe el DEC lo descifra con su clave privada. Obtiene así el dinero electrónico descifrado o descifrado (DED).

7. Después de descifrar la *cibermoneda* creada por el cliente con el *software* de gestión, el banco verifica la firma del cliente, la integridad del mensaje y los fondos del cliente.

8. El banco procede a atribuir un valor económico determinado al dinero electrónico creado. Este valor es simultáneamente descontado de la cuenta tradicional del titular, con lo que se obtiene el dinero electrónico valorado (DEV).

En caso de que no se verifiquen satisfactoriamente los datos indicados, la operación de creación de dinero electrónico quedará concluida.

9. Una vez obtenido el DEV es firmado digitalmente con la clave pública del cliente. Se reenvía el DEV al cliente por la red.

4.5.4. Requisitos para el empleo del dinero electrónico

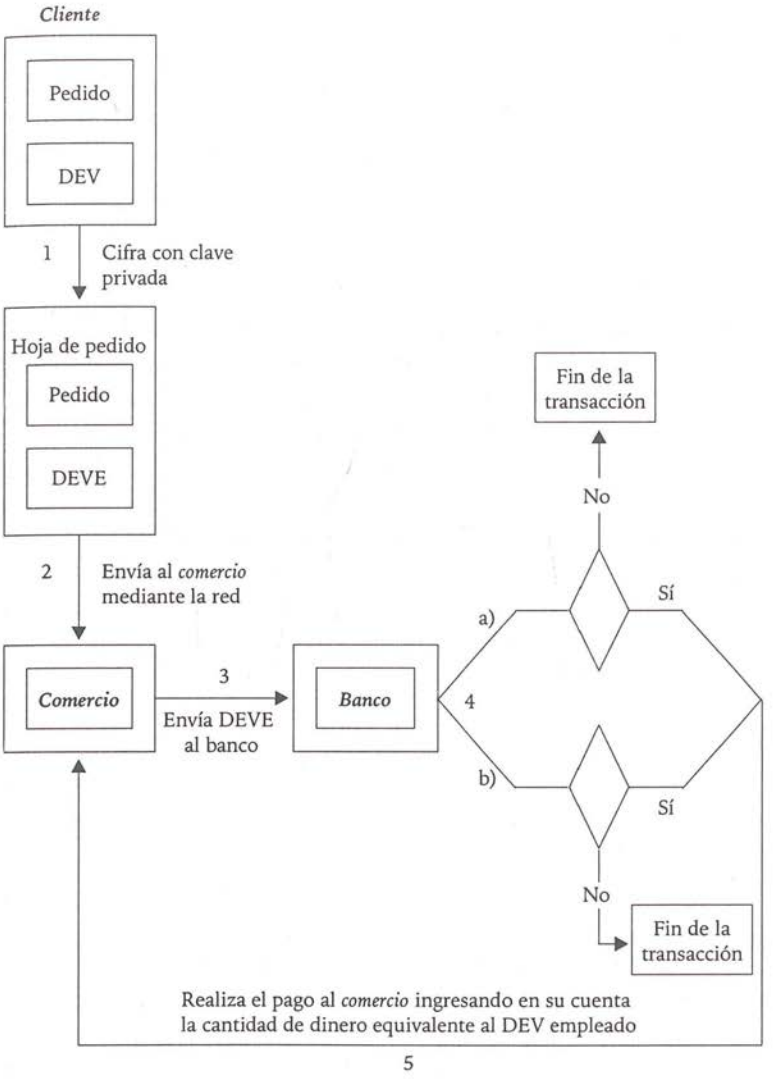
Para usar dinero electrónico es indispensable tener un *software* de gestión o pasarela de pagos. Además es necesario que todas las partes participantes (el banco emisor, el titular del dinero electrónico y el proveedor de servicios o bienes) posean una firma y un certificado digital.

4.5.5. Pago mediante dinero electrónico

El gráfico de la página 189 nos muestra el proceso del pago efectuado con dinero electrónico.

1. Llegado el momento del pago, el cliente cifra el DEV por el importe de la deuda. Obtiene así el dinero electrónico valorado cifrado (DEVE).

Pago efectuado con dinero electrónico



a) Verifica la autenticidad del DEV con clave privada del *banco*.
b) Verifica que el DEV no haya sido usado.

2. Una vez cifrado el DEV, el cliente envía por la red el DEVE y la información relativa al pedido al *comercio*.

3. El *comercio* envía el DEVE al banco emisor.

4. El banco emisor del dinero electrónico verifica la autenticidad de las *cibermonedas* (comprobación que realiza la entidad bancaria verificando la firma electrónica con la clave privada en las *cibermonedas* remitidas por el comerciante). Comprueba también que las *cibermonedas* no hayan sido usadas.

5. Si estos datos se comprueban, el banco emisor realiza en la cuenta del comerciante el depósito equivalente al valor del dinero electrónico empleado. Si la información no se verifica satisfactoriamente, la operación de pago con de dinero electrónico será finalizada.

A simple vista es fácil reconocer las ventajas que el *e-money* ofrece como modo de articulación del cumplimiento del pago. En efecto, se trata de un pago anónimo, sencillo, seguro y universalmente admitido. No obstante, también presenta dificultades que no deben ser obviadas. Entre ellas está el esfuerzo de las entidades bancarias que, con el fin evitar un doble uso del dinero electrónico, deberán almacenar el número de serie de cada *cibermoneda* gastada. Esta necesidad puede convertirse en una tarea imposible por la generalización de su uso, además del elevado costo en tiempo que significa la necesidad que tienen tanto el titular de las *cibermonedas* como el comerciante de estar en constante conexión con el banco.

4.5.6. Ventajas y desventajas en el empleo del dinero electrónico

Como afirma Rubén Hernández, el empleo del *e-money* tiene los siguientes beneficios:

> - **Disponibilidad.** El dinero electrónico está disponible las 24 horas del día, 7 días a la semana. Su utilización a través de redes electrónicas no tiene restricción de horario, ni de fines de semana u horas nocturnas, ni aún para operaciones entre sitios en diferentes países.
>
> - **Agilidad en operaciones.** El manejo interno (en bancos o similares) de la información asociada con el flujo de dinero ocurre de una forma más natural, pues la representación física (electrónica) del dinero es de la misma naturaleza que la información manejada por los sistemas:

bits. Se puede hacer uso directo de los datos, agilizando los procesos internos y los relacionados directamente con servicios al cliente.

- **Facilidad de recuperación.** El seguimiento y auditoria sobre las operaciones es más eficiente: controles y documentación se hacen —también— electrónicamente. Las facilidades para tener copias de respaldo, desautorizar una transacción o controlar el pago efectivo del dinero electrónicamente, conllevan toda una revolución frente a los mecanismos actuales. Imagine usted, que si pierde su dinero electrónico (p. ej. olvidó su clave secreta), pueda enviar a su banco electrónico la desautorización al pago efectivo de ese dinero (cancelación), e incluso, solicitar una copia del mismo pues en realidad no lo ha gastado y el banco lo puede corroborar.

- **Economía en producción a escala.** Aunque las primeras implantaciones de esquemas de dinero electrónico pueden requerir fuertes inversiones, el costo marginal de producción del equivalente a los billetes es cada vez menor. Una vez la infraestructura está montada, el esquema es menos costoso que la producción de papel moneda, o cheques.

- **Privacidad.** El uso y disponibilidad del dinero es menos evidente externamente. Ello crea un nivel de seguridad no existente, al menos con respecto al efectivo que se maneja tradicionalmente.

- **Acelera globalización.** La tan pronosticada «aldea global» recibe un paso más para su formación. Hoy es posible hacer compras en centros comerciales de Estados Unidos desde otros países, a través del World Wide Web, desde el PC de la casa.[81]

Del mismo modo, respecto de las ventajas del dinero electrónico, afirma Ortega Díaz citando a Martínez Nadal:

> [...] 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

[81] HERNÁNDEZ L., Rubén. «Dinero electrónico». En <http://www.aaapn.org/aaa/boletin/2000/pbol66a.htm>.

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).[82]

Como vemos, el dinero electrónico ofrece una serie de ventajas que permitirán superar las actuales ventajas del dinero en billetes o en moneda. Si bien es cierto que su implementación puede ser costosa e incluso insegura, una vez que se desarrolle y expanda la tecnología adecuada para su empleo los beneficios serán ampliamente superiores. En efecto, se trata de un medio de pago con un enorme potencial.

Las desventajas del uso del *e-money*, según Ortega Díaz, son las siguientes:

- **Carencia de estructuras de control**. Los procesos y operaciones alrededor de dinero electrónico son más nuevos que el concepto mismo; por ello, escapan a las estructuras actuales de control de bancos y entidades operadoras. Sin embargo, como se ha dicho anteriormente, el hecho de operar digitalmente favorece la rápida integración de esos controles de operación.

- **No hay regulación**. Si los procesos de operación interna apenas se están creando, la regulación del sistema externo (equivalente a las reglas de operación y reporte que establece la Superbancaria) ni siquiera se considera. El alcance e impacto que puede tener el dinero electrónico sobre los sistemas monetarios no se conoce totalmente; los problemas derivados del traspaso de fronteras sin regulación son discutidos bajo contextos académicos y de investigación, pero no se enfrentan de manera práctica aún.

- **Nuevos problemas de seguridad**. Muchos son excesivamente pesimistas ante la posibilidad de «huecos» de seguridad generados por los nuevos mecanismos. Es claro que por tener bases diferentes, se requieren elementos de control y seguridad nuevos; pero esto es diferente a afirmar que sea una debilidad intrínseca del dinero electrónico. La evolución tecnológica contribuye también al desarrollo de los mecanismos de seguridad y el estar implementados sobre datos y procesos digitales favorece su implantación.

[82] ORTEGA DÍAZ. Ob. cit.

- **Susceptibilidad a manipulaciones criminales.** Este punto es un caso particular del anterior, solo que en este caso se enfrenta un tipo de criminalidad distinto al tradicional. Algunos problemas de seguridad actuales son eliminados con los esquemas de dinero electrónico; ocurre ahora, que se requieren niveles más sofisticados de criminalidad basados en conocimiento avanzado de la tecnología. Es menos probable encontrar este perfil de criminales, pero uno solo que sea exitoso, puede causar daños catastróficos que lleven a una pérdida de confianza en el sistema o en su moneda. Por esta razón, hoy solo vemos aplicaciones de dinero electrónico en ambientes fáciles de controlar: por su tamaño, por lo cerrado de la comunidad beneficiada, o por poco riesgo en bajos volúmenes de las transacciones; no es la tecnología la que impone el límite.

- **Proceso de globalización.** De lo dicho, es claro que aunque la globalización del comercio electrónico es una tendencia soportada en parte por la evolución tecnológica, ella no se da sin resolver problemas serios y retos grandes de organización y operación; ésta es la razón por la cual no estamos ya haciendo uso expandido de estos medios. La eficiencia de una sociedad está ligada a la competitividad de sus estructuras; sin una adecuada velocidad de adopción de medios tecnológicos, el retraso es cada vez mayor frente a quienes sí lo hacen; es como la diferencia entre una fábrica que produce un carro en un mes y la que puede hacerlo en cinco días (el retraso aumenta con cada día).[83]

Las desventajas señaladas están relacionadas con el empleo relativamente reciente del dinero electrónico y con su implementación tecnológica y legal. Como indicamos al momento de comentar las ventajas de este medio de pago electrónico, estas desventajas se deben a la fase de implementación en la que se encuentra el dinero electrónico. Consideramos que se reducirán considerablemente una vez que este medio de pago esté más ampliamente implementado. Por otro lado, si bien es cierto que podrá ser susceptible a manipulaciones criminales, no lo es más que el dinero representado en billetes o monedas.

---

[83] HERNÁNDEZ. Ob. cit.

En conclusión, al poner en la balanza las ventajas y desventajas del dinero electrónico, consideramos que se inclina a favor de su utilización. En efecto, una vez realizada la implementación legal y tecnológica, las ventajas superarán ampliamente a las desventajas.

4.6. Pagos mediante teléfono móvil

4.6.1. Introducción

Iniciamos el análisis del sistema de pago mediante el teléfono móvil con estas palabras de Javier Santomá.

> Se cree que en Europa la nueva expansión, que a su vez le permita reducir distancias con respecto a Estados Unidos en el uso de Internet, será la introducción de la telefonía móvil como conductor de las transacciones de las operaciones en la red. Indicado para compras en Internet o en determinadas transacciones del mundo real, como el pago de taxis.

La generalización del teléfono móvil en estos últimos cuatro años, como señala Ortega Díaz,[84] es lo que ha llevado a algunas empresas telefónicas a desarrollar sistemas de pago basados en el habitual teléfono móvil, con la meta de obtener sistemas seguros y rápidos.

4.6.2. Ventajas del pago mediante teléfono móvil

Una de las principales ventajas de este modelo es que no es necesario instalar un *software* ni un *hardware* específico; en efecto, su funcionamiento es muy sencillo. Las operadoras de teléfonos deberán crear nuevas aplicaciones y contenidos o bien buscar alianzas. En otras palabras, será necesario entrar en nuevas áreas de negocio. Como requisito para el empleo de este sistema, tanto el comprador como el vendedor deberán estar abonados al sistema diseñado para ello.

---

[84] ORTEGA DÍAZ. Ob. cit.

4.6.3. Funcionamiento del pago mediante teléfono móvil

El funcionamiento del sistema es el siguiente. En el momento de pagar se introduce el número de teléfono en la casilla indicada en la pantalla del ordenador, o bien en el terminal electrónico del punto de venta de la que dispone el vendedor. A continuación el sistema electrónico genera una llamada telefónica al usuario, que le comunica el importe y le pide que autorice la transacción introduciendo su PIN (clave). Finalmente, el usuario introduce el PIN, con lo que autoriza la operación de pago.

Se trata de un sistema seguro, ya que la operación se realiza mediante la red telefónica y no es necesario introducir el número de la tarjeta en Internet. Además de la seguridad, el factor clave para su expansión es la simplicidad de su uso. La idea es que un futuro la técnica sea aplicable a otros dispositivos móviles y en las nuevas agendas electrónicas.

4.6.4. Tipos de pago móvil

Un ejemplo de la aplicación del sistema de pago móvil es el dispositivo llamado CoCyph, que funciona como una tarjeta prepago. El cliente escanea el código de barras de los productos que quiere adquirir, mediante un lector incluido en el dispositivo. La información es enviada por teléfono, vía Internet, a un centro de operaciones, en el que el dinero depositado previamente por el cliente en una cuenta es transferido a la cuenta del comercio. Al mismo tiempo se envía un mensaje al cliente para que confirme la compra.

Otros modelos plantean la posibilidad de cargar las compras realizadas en Internet a la factura del teléfono, sea fijo o móvil.

4.6.5. Modalidades del pago móvil

Según Ortega Díaz,[85] son dos las modalidades de pago por sistema móvil.

---

[85] Ibíd.

■ **Pago móvil con tarjetas prepago**

El sistema es especialmente sencillo.

- El usuario adquiere una tarjeta prepago en cualquiera de los establecimientos autorizados por la compañía prestadora del servicio.
- Una vez 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, que 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. Procederá a autorizar el pago si el precio del bien o del servicio es inferior al saldo remanente en la tarjeta prepago.
- Si el pago es autorizado, el titular recibirá una factura electrónica en la que se le indicará la información acerca del bien adquirido y el precio pagado.

Este sistema tiene ventajas indudables: es seguro, confidencial, anónimo y completamente electrónico. No obstante, no es una solución global por dos causas fundamentales. En primer lugar, 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 solo 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. En segundo lugar, es un medio destinado a satisfacer pagos de escaso valor. Esta característica lo convierte en una solución válida y eficaz al problema de los micropagos, pero hace imposible el pago de bienes y servicios de importe elevado.

■ **Pago móvil basado en el pago indirecto con tarjeta de crédito**

El pago de bienes y servicios de costo elevado es solventado mediante esta modalidad de pago móvil. No obstante, a diferencia de lo que sucede en el caso anterior, no se realiza únicamente en la red. Esta característica lo desvirtúa, en buena medida, como medio de pago. El procedimiento es el siguiente:

- Es necesario convertirse en titular de una tarjeta de crédito. Con ella 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.
- Una vez elegido el comerciante y el producto, se selecciona el pago móvil como modalidad de pago. A continuación se introduce el número del teléfono y se confirma que se desea efectuar el pago.
- Finalmente y dentro de un período de 24 horas, el usuario debe contactar telefónicamente a la empresa suministradora del servicio de pago para confirmar, mediante la comunicación del PIN, la autorización del pago. Si se confirma, la empresa autoriza y hace efectivo el pago por los medios tradicionales de pago con tarjeta.

Como vemos, si bien esta segunda modalidad hace posible el pago de importes elevados, presenta serios inconvenientes:

- Es una solución que sigue sin ser global. El usuario solo tiene la posibilidad de contratar con los comercios adheridos a la empresa prestadora del servicio de pago.
- No es confidencial. Todos los participantes en el pago conocen el precio y el bien o el servicio contratado.
- No es anónimo, por lo que el banco puede elaborar un perfil de los gustos y hábitos del comprador.

4.7. Principales medios de pago electrónico en el mercado mundial

Hemos descrito los principios de funcionamiento de los medios de pago principales. Ahora nos referiremos a los medios de pago electrónicos que se han desarrollado en el mercado mundial y que reúnen las características que hemos indicado. Sin bien ninguno de estos sistemas de pago tiene aplicación en nuestro país, los mencionamos a modo de ilustración para tener una idea de cuáles son los sistemas que se emplean y cómo funcionan.

4.7.1. Sistemas card-based

Los estudios que analizan las conductas de sus poseedores han constatado el hecho de que en la mayoría de los casos el dinero electrónico se utiliza para transacciones de bajo valor. Este hecho es precisamente lo que limita su expansión. En efecto, para facilitar estas transacciones de bajo valor se requiere de una fuerte inversión inicial en lectores de tarjetas (terminales en puntos de venta) al servicio de los comercios, así como una infraestructura para controlar y consolidar.

En el *Survey of Electronic Money Development*, último informe publicado por el Bank of International Settlements (BIS) sobre dinero electrónico, que analiza el desarrollo de este tipo de productos y soluciones en numerosos países, queda patente que los líderes en el desarrollo de soluciones *card-based* son Visa, con Visa Cash, y Mondex, iniciativa desarrollada por MasterCard (véase el cuadro 1).

4.7.2. Sistemas software-based

Los sistemas *software-based* están menos desarrollados y, en muchos casos, todavía se encuentran en fase de prueba. Los primeros proyectos surgieron a mediados de los noventa, pero no llegaron a prosperar. Se intentó crear una auténtica moneda virtual, y en la actualidad aún se utiliza la tecnología creada por DigiCash como pionera en soluciones de pago por Internet (véase el cuadro 2).

4.7.3. Sistemas por puntos

Otro tipo de sistema *software* es el pago por puntos (véase el cuadro 3). Con la misma idea de crear una moneda de Internet surgieron productos que utilizan un soporte *software*, aunque todavía no es posible hablar de una nueva forma de dinero, ya que su validez se limita a la red.

Se trata básicamente de un sistema virtual de incentivos o puntos en el que un usuario es gratificado con una moneda (puntos) que le permite hacer compras en el mercado virtual electrónico. El modelo es idéntico al de las tradicionales millas o puntos que ofrecen las compañías aéreas con sus tarjetas de fidelización.

4.7.4. Sistemas e-mail money

El *e-mail money* es un valor cifrado por el que primero se paga en el mundo real (mediante una tarjeta de crédito o en efectivo) y que más tarde se utiliza para comprar en la red.

El sistema es, sin duda, más una instrucción de cómo se debe pagar que una nueva forma de dinero, y supone un avance significativo. En el mercado hay diferentes empresas que se distinguen en su enfoque (véase el cuadro 4).

Cuadro 1
Sistemas *card-based*
Productos y características

Visa Cash. Utiliza tarjetas con circuito integrado (*smart cards*). Permite hacer pagos con tarjeta de crédito, así como con el dinero electrónico almacenado en ellas. El dinero puede ser un sustituto del efectivo en compras de pequeño valor y en cajeros automáticos. Hay dos tipos de tarjetas disponibles: las desechables y las recargables.

Modex. Es la apuesta del consorcio MasterCard International para el desarrollo de tarjetas monedero multiplicación (*smart-cards*). Se puede utilizar en establecimientos tradicionales o virtuales, como Internet y televisión digital. El valor se transfiere directamente de un chip a otro, y no hay terceros involucrados en la transacción. La tarjeta chip permite que el dinero almacenado en el monedero electrónico pueda estar disponible hasta en cinco divisas diferentes. Además, permite tener un registro de las diez últimas transacciones realizadas y poner un código de acceso para bloquearla.

Blue. La última apuesta desarrollada en Estados Unidos ha tenido un notable éxito. Se trata de la tarjeta Blue, desarrollada por American Express. Es una clásica tarjeta de crédito, con un dispositivo chip incorporado. Es posible acceder en la red a todos los movimientos realizados con la tarjeta. Además, ofrece un sistema de fidelización automático. Dispone de un monedero virtual para realizar compras en Internet. El cliente recibe un lector de *smart-card*, que se añade al ordenador. En el momento de realizar una compra en Internet, se inserta la tarjeta en el lector y se teclea el número secreto o PIN.

Internet Cash. Muy popular en Estados Unidos, se trata de un sistema prepago en el que las tarjetas se compran en comercios tradicionales. Existen tarjetas disponibles con denominaciones desde 10 hasta 100 dólares. Una vez que se posee la tarjeta se debe visitar el sitio web de Internet Cash para activar y crear una clave secreta, sin tener que proporcionar ningún dato personal. Con la tarjeta activada es posible realizar compras por Internet en todos los comercios que acepten el sistema.

Cybermoda. Tarjeta prepago que puede adquirirse en comercios. Contiene una serie de 16 dígitos (como las tarjetas bancarias tradicionales) a modo de certificado. El certificado tiene un valor depositado en dólares igual al importe pagado por él. Se activa mediante su página web. A partir de ese momento, el importe de la tarjeta o certificado se añade al saldo de la cuenta. Las compras se realizan en su sitio web. También pueden adquirirse estos certificados con valor en su sitio web, pagando con tarjeta de crédito o con un cheque.

Cuadro 2
Sistemas *software-based*
Productos y características

Ecash. Ofrecido por Deustche Bank en Alemania. Sistema de pago electrónico que se puede utilizar en Internet para comprar bienes y servicios. El usuario debe instalar un *software* en su ordenador, llamado *ecash wallet*. Este monedero electrónico permite que el consumidor se comunique con el comerciante y con el banco. Al incorporarse al sistema se abre una cuenta en el Deustche Bank. El usuario podrá realizar transferencias a esta cuenta para disponer de fondos para sus compras en Internet. En el momento en que dispone de fondos, el valor de la cuenta queda depositado en la *ecash wallet* como dato cifrado. Esta característica impide que accedan a esta información quienes no participan en el sistema. En el momento de la compra, la transferencia se realiza directamente a la *ecash wallet* del comercio, y posteriormente al Deustche Bank, que ejerce de compensador de los pagos.

Kleline. Filial del grupo francés BNP-Paribas creada para garantizar las transacciones en Internet. Ha desarrollado una idea similar a las tarjetas monedero, la K-wallet, pero en forma de cuenta monedero virtual. BNP-Paribas ha decidido abandonar el desarrollo comercial de Kleline, aunque continuará con la idea del monedero virtual.

Cuadro 3
Sistemas de puntos
Productos y características

Beenz.com. Empresa líder del mercado. Los consumidores son premiados por realizar algún tipo de *e-work* en la red, como visitar determinada página web, interactuar con algún negocio en la red, participar en encuestas, comprar o simplemente acceder a Internet mediante un servidor determinado. En su página web se encuentran las empresas adheridas al sistema y que gratifican a quienes visitan sus páginas. El sistema ya es operativo en un gran número de países, entre ellos España. También es posible ser gratificado por compras tradicionales en línea con una clásica tarjeta de fidelización (*Rewardzcard*). Además, los puntos obtenidos pueden transferirse a la tarjeta y adquirir bienes, aunque este servicio está restringido a Estados Unidos y Canadá.

El valor de transferencia es de 200 beenz a un dólar. La tarjeta es efectiva en la mayoría de establecimientos que aceptan la tarjeta MasterCard. La empresa vende su «moneda» a los comercios asociados y es así como logra sus beneficios. El sistema se instala en los comercios que lo aceptan. La instalación es muy sencilla y rápida. Cada comercio decide la gratificación que dará a sus clientes. El problema con este tipo de modelo es que, al no ser convertible, no se puede considerar realmente dinero digital.

Cybergold. Cybergold va un poco más allá y permite convertir el montante de dólares Cybergold en dólares reales. Actualmente se puede gastar los Cybergold acumulados de tres maneras: se puede donarlos a una ONG, transferirlos a la tarjeta Visa o MasterCard o ingresarlos directamente en una cuenta corriente. El sistema solo es operativo en Estados Unidos y Canadá. No hay un límite de Cybergold para canjear por dólares reales, pero la empresa advierte que, lógicamente, el número de empresas que podrán adherirse al sistema es limitado. Si un usuario quiere realizar una compra y no dispone de puntos suficientes, puede completarlos pagando con tarjeta.

Zakis. Primer modelo surgido en España. Un Zaki equivale a una peseta (1 euro equivale a 166.386 pesetas). Se puede gastar en cualquiera de los comercios en línea asociados y puede utilizarse como forma parcial o total de pago. Se ganan navegando en Internet, participando en encuestas y sorteos o comprando en la red. Se gasta en cualquiera de las tiendas asociadas al sistema. Los Zakis se pueden usar como forma de pago total o parcial.

Cuadro 4
Sistemas *e-mail money*
Productos y características

Paypal es líder de su segmento en transacciones P2P y una de las empresas más consolidadas. Se trata de un servicio prepago para la disposición de efectivo (al igual que Flooz). Después de abrir una cuenta en su página web se puede enviar dinero por correo electrónico a cualquier persona que tenga una dirección de correo electrónico. Incluso es posible transferir dinero desde una agenda electrónica tipo Palm a otra, mediante señales infrarrojas. Para realizar la transferencia se puede pagar con tarjeta de crédito o mediante una cuenta corriente. El servicio ya está disponible en numerosos países. Uno de sus puntos débiles es la ausencia en los comercios de mecanismos contra el fraude, que sí existen en el caso de las tarjetas de crédito.

E-Count. Tarjeta de débito MasterCard. Al transferir fondos desde una cuenta permite disponer de efectivo en un cajero E-count, también conocido como la cuenta personal. Este modo de pago utiliza una tecnología que básicamente proporciona una tarjeta de débito MasterCard (de 16 dígitos, como las tradicionales) tan pronto como los fondos son transferidos por el titular a su cuenta, o bien a un beneficiario, mediante un tercero. A diferencia de algunos de sus competidores, no está limitado a transacciones en línea y se puede disponer del dinero desde un cajero utilizando la tarjeta. Las características de la cuenta varían según las características de gasto de su titular.

E-Gold. Ofrece un servicio parecido, pero lo que se transfiere es valor en metales preciosos. Los clientes abren una cuenta en la red comprando oro u otros metales preciosos y el valor de la cuenta se registra en la moneda e-gold. Cuando se quiere realizar una transferencia se transfieren gramos del metal adquirido insertando el número de cuenta del receptor y una contraseña. Este servicio, debido a su visión del riesgo financiero, prefiere apoyarse en un activo físico, con lo que el único riesgo al que queda sujeto el usuario es el del tipo de cambio.

4.8. Conclusiones

1. Para los fines de este estudio consideramos medios de pago electrónicos aquellos instrumentos que permiten extinguir la obligación de dar una suma de dinero —contraída o no por medios electrónicos— mediante la transferencia de fondos de propiedad del deudor en favor de su acreedor.

2. La seguridad en el empleo del dinero digital es un aspecto medular en el comercio electrónico, ya que se encuentran en juego los recursos económicos con los que se realizan las transacciones económicas en Internet.

El concepto de seguridad en el pago por medios electrónicos está relacionado al sistema de pagos que se emplee. Entendemos como sistema el conjunto de elementos (*software, hardware,* información, titulares de medios de pago, entidades financieras y proveedores de bienes y servicios) que interactúan para dotar de seguridad a los medios de pago electrónicos. Por este motivo, las amenazas al sistema pueden ser externas o internas.

3. Los objetivos de la seguridad en el sistema de pagos electrónicos son básicamente asegurar que cualquier servicio del sistema de dinero digital esté disponible a los usuarios cuando lo piden y que sea destinado al fin que ellos elijan.

4. Los medios de pago electrónico tienen una doble naturaleza jurídica: son, por un lado, un medio de extinción de obligaciones y, por otro, un medio de seguridad jurídica en el comercio electrónico.

5. Los medios de pago electrónicos, de acuerdo con el nivel en que se sirvan de Internet, pueden ser clasificados como medios de pago independientes, medios de pago dependientes parcialmente y medios de pago dependientes totalmente.

6. Los medios de pago que tienen más trascendencia en el comercio electrónico son la tarjeta electrónica, el dinero electrónico y el pago mediante teléfono móvil.

7. La tarjeta electrónica

- La tarjeta electrónica es un medio de pago cuyo funcionamiento está basado en la transferencia de fondos. Pese a que

tienen distintas denominaciones, nos parece conveniente llamarlas «tarjetas electrónicas», pues consideramos que actualmente todas las tarjetas incorporan elementos electrónicos para funcionar en las redes de pago electrónico.

- Existen diversos criterios de clasificación de las tarjetas: según la tecnología incorporada a la tarjeta (tarjetas tradicionales o nuevas tarjetas) y según la forma de liquidación de las disposiciones realizadas (tarjetas de crédito, tarjetas de débito, tarjetas de cargo diferido o tarjetas prepagadas).
- Los sujetos participantes en un pago realizado en el comercio electrónico mediante una tarjeta electrónica son el emisor de la tarjeta, el titular, el proveedor aceptante, el servidor del emisor, el servidor del titular, el servidor del proveedor aceptante y el prestador de servicios de certificación. Además, interviene la empresa propietaria de la marca que autoriza la emisión de la tarjeta en régimen de franquicia o licencia de uso, según el caso.
- Para que una operación de pago realizada con tarjeta electrónica sea válida se requerirá, en primer lugar, que se admita el medio de pago como tal. En segundo lugar, se debe tener en cuenta si se trata de una operación de compraventa simple (realizada sin la intervención de una entidad de certificación, con lo cual la aceptación de una transacción y su correspondiente pago se realiza mediante un formulario de pedido) o de una operación en la que interviene una entidad de certificación.
- Los efectos del cumplimiento de una obligación de pago se deben considerar de acuerdo con el tipo de tarjeta electrónica empleada. En efecto, el pago realizado mediante una tarjeta electrónica de crédito produce principalmente efectos liberatorios para el titular de la tarjeta pero no para el emisor, quien por virtud del contrato de emisión se obliga a garantizar el pago de las obligaciones contraídas mediante tarjetas por el titular. El pago con tarjetas electrónicas de débito produce todos los efectos del pago: el titular se libera de la obligación extinguiéndola y satisfaciendo al acreedor, quien

recibe el importe de la deuda por vía electrónica en su cuenta. El pago realizado con tarjetas virtuales, por su parte, produce los mismos efectos del pago efectuado en dinero efectivo. En otras palabras, se satisfacen los intereses del acreedor, la deuda se extingue y el deudor se libera de su obligación.

- En las compras que requieren una operación de comercio electrónico simple las pruebas son los formularios de pedidos enviados por el cliente. En ellos consta el número de unidades solicitadas, su identificación, los datos de la tarjeta, el precio, los gastos de envío y los datos requeridos para la entrega: dirección postal y teléfono de contacto.

  En el pago con tarjetas electrónicas la prueba es la factura electrónica. Aun cuando en nuestro ordenamiento jurídico no se ha regulado la emisión de facturas electrónicas, es posible recurrir a las disposiciones de la Convención de Viena sobre Compraventa Internacional de Mercaderías para el empleo de registros computarizados como elementos probatorios.
- Para garantizar la efectividad de los medios de pago en Internet, así como la protección de la información de los sujetos transmitida en la red, se han desarrollado determinados protocolos o procedimientos. Estos protocolos emplean la criptografía y la función de certificación. Los principales son el SET y el SSL.

  El protocolo SET garantiza la confidencialidad de la información, tanto la económica como aquella relacionada a los bienes comprados, pues permite cifrar separadamente la información. Ofrece servicios de autenticación (todas las partes pueden autenticarse mutuamente mediante certificados electrónicos), confidencialidad (la información sobre los datos de compra y la tarjeta se transmiten cifrados), integridad (se garantiza la inalterabilidad del mensaje) y gestión de pagos (con autorizaciones y liquidaciones de pagos).

  Para el empleo del protocolo SSL, en cambio, el usuario solo llena un formulario en el que hace constar sus datos personales y bancarios. Mediante un canal seguro los datos

son cifrados con criptografía simétrica y enviados al comerciante, que los recibirá y los descifrará, para luego ejecutar el pago en la entidad bancaria correspondiente.

8. El dinero electrónico

- El dinero electrónico, también llamado *e-money* o *cybermoneda*, es la representación de un valor abstracto por medios electrónicos, respaldado por una autoridad pública, y que permite la realización de todo tipo de transacciones patrimoniales.
- En la creación del dinero electrónico deberán intervenir la persona que quiere emplear este medio de pago, un banco emisor del dinero y un proveedor de bienes y servicios que acepte este medio de pago. Se requiere, además, de un *software* desarrollado especialmente. En la creación del dinero electrónico no es necesaria la intervención del Estado para dotarle de eficacia para la extinción de las obligaciones. Esta eficacia proviene de un vínculo contractual entre los diversos sujetos participantes en su creación y en su empleo.
- La intervención del Estado en la creación de dinero electrónico deberá ser indirecta, al autorizar, supervisar y fiscalizar a las entidades financieras que se dediquen a esta actividad. Este hecho se debe a la intención de minimizar la participación del Estado en el comercio electrónico, pues le falta la flexibilidad necesaria para adaptarse a los avances tecnológicos y las nuevas formas de entablar y concluir relaciones comerciales.

9. Pagos mediante teléfono móvil

- El pago mediante teléfono móvil surge como una opción debido al auge de las comunicaciones mediante teléfonos móviles, y debido a la necesidad de garantizar una mayor seguridad para las transacciones comerciales realizadas en la red.

  La ventaja principal de este modelo es que no necesita instalar un *software* o un *hardware* específicos. Su funcionamiento es muy sencillo.
- El funcionamiento de este sistema de pago se basa en la introducción de una clave en el momento en que se realiza una llamada telefónica al teléfono móvil para autorizar la

transacción realizada. De esta manera, se garantiza la seguridad de la información del usuario, pues no es necesario introducir el número de la tarjeta de crédito en la red. Existen diversos tipos de pagos por móvil, todos basados en el principio de funcionamiento descrito.

4.9. La biometría

4.9.1. Introducción

Como hemos analizado, los distintos medios de seguridad señalados proporcionan un nivel de seguridad que permite un desarrollo aceptable del comercio electrónico. Garantizan la identidad de las partes, la integridad de los mensajes y la efectividad del pago realizado por medios electrónicos, además de impedir la repudiación de los mensajes.

Sin embargo, estos medios de seguridad no ofrecen una seguridad absoluta. La biometría aparece entonces como el medio de seguridad más efectivo para el desarrollo del comercio electrónico, como veremos más adelante.

La biometría es la técnica de identificación más antigua. Los perros tienen ladridos distintos; los humanos reconocen las caras de los demás; en el teléfono se reconoce la voz de la persona que está en la línea; en un contrato, la firma identifica a la persona que lo rubricó; una fotografía identifica a la persona poseedora de un pasaporte determinado.[86] Como vemos, la identificación de las personas a partir de sus rasgos fisiológicos ha sido siempre practicada y es la primera opción para identificar a una persona.

Como vemos, la biometría es la forma de identificación más sencilla que pueda existir. Sin embargo, su aplicación en el *e-commerce* se complica por las razones que más adelante mencionaremos.

---

[86] «Biometría: verdades y ficciones». Traducción de Ángel Galindo. En <http://www.kriptopolis.com/criptograma/0004_5.html>.

4.9.2. Definición de biometría

A continuación mencionaremos algunas definiciones del medio de seguridad que estamos estudiando.

De acuerdo con González Rodríguez «[...] surge la biometría, también conocida como técnicas de identificación biométrica, con el objetivo de resolver este problema a partir de características que son propias de cada individuo, como voz, huella dactilar, rostro, etc.».[87]

Otra definición la encontramos en el documento denominado *De la contraseña a la identificación biométrica*: «[...] medición de distintas características físicas exclusivas y determinantes de la identidad de un individuo, como las huellas dactilares o el iris».[88]

Nosotros definimos la biometría como el medio tecnológico que tiene por objeto lograr la identificación de una persona, a partir de una o más de sus características fisiológicas.

Esta definición recoge el principio de equivalencia funcional, pues incluye toda tecnología que recoja cualquier característica fisiológica de una persona. Este hecho obedece a que la biometría puede asociar prácticamente cualquier parte del cuerpo humano con una clave para verificar la identidad del usuario.

4.9.3. Características de la biometría

- Es el medio de seguridad para la identificación de personas de mayor antigüedad.
- Su función en el comercio electrónico es garantizar la identidad de los sujetos que participan.
- Su funcionamiento se basa en la identificación y en la individualización de las personas mediante sus rasgos fisiológicos, como la retina y las huellas digitales, entre otros.

---

[87] GONZÁLEZ RODRÍGUEZ, Joaquín. «Identificación biométrica». En <http:// www.iec.csic.es/criptonomicon/articulos/expertos73.html>.

[88] «De la contraseña a la identificación biométrica». En <http://www.tecnipublicaciones.com/teleinf/actualidad/seguridad.asp?opcion=informe>.

- Es un medio de seguridad que ofrece la mejor de las garantías con respecto a la identificación de las personas, pues los rasgos fisiológicos son muy difíciles de imitar.
- Está íntimamente vinculado a los soportes tecnológicos que permiten la lectura de los rasgos fisiológicos para la identificación.
- Tomando en consideración el actual desarrollo tecnológico, este medio de seguridad es de difícil implementación debido a sus altos costos.

4.9.4. Ventajas y desventajas del empleo de la biometría

La principal ventaja de este medio de identificación de los sujetos que participan en una operación de comercio electrónico es que los rasgos fisiológicos (unos más que otros) son únicos y no pueden ser sustraídos, a diferencia de lo que ocurre con las claves empleadas en el sistema de criptografía.

Sobre esta ventaja afirma González Rodríguez:

> Estas técnicas de identificación biométrica, frente a otras formas de autenticación personal como el uso de tarjetas o PINes (Personal Identification Number, o número de identificación personal, como el usado en cajeros automáticos), tienen la ventaja de que los patrones no pueden perderse o ser sustraídos, ni pueden ser usados por otros individuos en el caso de que lleguen a tener accesible nuestra tarjeta personal o PIN. Debemos tener en cuenta que gran parte de los sistemas de autenticación actuales están basados únicamente en el uso de una tarjeta personal o un PIN. Así, por ejemplo, es habitual que en el caso de pérdida o sustracción de una cartera, cualquiera pueda hacerse pasar por uno mismo, ya que es extremadamente frecuente tener junto a las tarjetas personales, el/los número/s secreto/s (PINes) apuntado/s en la misma. Éste problema de suplantación de identidad quedaría totalmente resuelto con el uso de patrones biométricos como medio de autenticación personal .[89]

[89] GONZÁLEZ RODRÍGUEZ. Ob. cit.

Sin embargo, la biometría presenta un inconveniente que por el momento obstaculiza su desarrollo como medio de seguridad jurídica en el comercio electrónico. Este inconveniente es el elevado costo de la implementación de la tecnología necesaria, pues se requiere de una infraestructura mucho más avanzada que la necesaria para el empleo de la criptografía y para la función de certificación.

No obstante, esta desventaja es temporal. En efecto, con el avance de la tecnología se logrará implementar soportes tecnológicos que permitirán superar este obstáculo.

Otro posible inconveniente es que las características fisiológicas pueden cambiar con el tiempo. Esta dificultad se puede superar debido a que la biometría puede analizar las distintas características fisiológicas que no cambian.

En conclusión, podemos afirmar que existe un balance a favor de las ventajas de este medio de seguridad. Cualquier crítica a este medio de seguridad es tan válida como la que se haga a cualquier otro de los medios de seguridad que hemos estudiado, por lo cual este medio no debe ser descartado.

4.9.5. Técnicas de autenticación biométrica

Hemos elaborado el siguiente cuadro a partir de las afirmaciones de González Rodríguez[90] para describir las técnicas de autenticación biométrica más extendidas y aplicables. Además, evaluaremos sus características fundamentales en términos de precisión (P), costos (C), aceptación por parte del usuario (A) y grado de intrusión de la técnica, es decir, vulnerabilidad del sistema (I). Obviamente, la técnica ideal debe tener un grado máximo de precisión y aceptación y un grado mínimo de coste e intrusión (P++++, C+, A++++, I+).

[90] Ibíd.

Principales técnicas de autenticación biométrica

Técnica de autenticación	Funcionamiento	Precisión	Costos	Aceptación por el usuario	Intrusión en la técnica
Reconocimiento de huella dactilar	El usuario solo tiene que situar la yema de un dedo (normalmente el índice) sobre un escáner de huella.	++++	++	+++	++
Reconocimiento facial	El sistema dispone de una cámara que graba al usuario y analiza su rostro.	++	+++	++	+
Reconocimiento de voz	La persona pronuncia un código de acceso prefijado (nombre o apellidos, DNI, número de teléfono, PIN, etc.) o una frase diferente cada vez por invitación del sistema («diga usted...»). Es reconocido por el sistema a partir de las características de la voz que grabó en el momento del acceso.	+++	+	++	+
Reconocimiento de la forma de la mano	La persona pone su mano abierta sobre un escáner específico. Es reconocida a partir de la forma y geometría de la mano.	++	+++	++	++
Reconocimiento del iris	El sistema obtiene una imagen precisa del patrón del iris del individuo y lo compara con el patrón previamente guardado del usuario.	++++	++++	+++	+++
Reconocimiento de firma	El individuo firma sobre una superficie predeterminada. La firma es verificada frente a un patrón obtenido previamente de la misma persona.				

Como señala González Rodríguez, sea cual sea la técnica seleccionada para una determinada aplicación, tendremos que ponderar sus restricciones o peculiaridades frente al grado de seguridad añadido que tenemos y del que antes carecíamos. Estas características son básicamente los siguientes aspectos:

- Necesidad de un dispositivo de adquisición específico en el que esté el usuario (lector de huella dactilar, micrófono, cámara, etc.).
- Posible variación con el tiempo del patrón a identificar (afonías o catarros en el caso de la identificación de la voz o el uso de gafas, bigote, barba, entre otros, en el caso de la identificación a partir de rasgos faciales.
- Probabilidad de error individual de cada una de las técnicas (entre uno por cien y uno entre varios millones, dependiendo de la técnica elegida).
- Aceptación por parte del usuario de cada una de las técnicas, en función de si son intrusivas, si son cómodas, si protegen la privacidad (al menos en apariencia), si son sencillas de usar, etc.

De este modo, dependiendo de la situación en que necesitemos realizar una autenticación segura del usuario buscaremos cuál es la técnica biométrica (o la combinación de técnicas) más adecuada, en función de los cuatro parámetros fundamentales anteriormente mencionados.

4.9.6. Naturaleza jurídica de la biometría

Se trata de un medio por el cual se logra la identificación casi indubitable de una persona para su vinculación jurídica con otras. Por ende, es un medio de seguridad jurídica en el comercio electrónico.

4.9.7. Viabilidad de la biometría para formar parte del sistema de seguridad jurídica en el comercio electrónico

Consideramos que la biometría es el medio ideal para identificar a una persona. Por lo tanto, creemos que garantiza la eficacia jurídica de los actos que se realicen en Internet. La biometría haría

innecesarios los sistemas de criptografía asimétrica o simétrica y el empleo de la función de certificación para garantizar la identidad de los sujetos e impedir la repudiación de los mensajes. En efecto, la comprobación de la identidad de una persona mediante sus rasgos fisiológicos sería suficiente para garantizar esta información.

Sin embargo, como hemos señalado, la biometría aún no se ha introducido plenamente como un medio de identificación. Más aún, hasta el momento ha sido desplazada por otros sistemas de seguridad, como la criptografía —asimétrica o simétrica— o las entidades de certificación.

Por este motivo, en este estudio, no consideraremos la biometría como un componente del sistema de seguridad jurídico en el comercio electrónico. Dejamos constancia, sin embargo, que esta exclusión se debe a la momentánea dificultad de su incorporación e implementación a dicho sistema.

4.10. Conclusiones

1. La biometría es un medio de seguridad jurídico en el comercio electrónico que permite la identificación de una persona mediante sus rasgos fisiológicos. Es el sistema más preciso para hacer frente al problema jurídico de identificación de las partes en una operación de comercio electrónico.

2. Pese a ser el medio más preciso e infalible que existe para la identificación de una persona por ser los rasgos fisiológicos de muy difícil imitación, aún no tiene una implementación muy difundida en el *e-commerce*. Por lo tanto, los medios de identificación se basan actualmente en la criptografía y en la función de certificación.

3. Los principales medios de autenticación biométrica son los siguientes:

- reconocimiento de la huella dactilar
- reconocimiento facial
- reconocimiento de la voz
- reconocimiento de la forma de la mano

- reconocimiento del iris
- reconocimiento de la firma

5. CONCLUSIONES DEL CAPÍTULO

1. Los medios de seguridad jurídica en el comercio electrónico permiten entablar transacciones comerciales en Internet de una manera confiable y oponible a terceras personas. Esta característica incentiva la participación en el comercio electrónico.

2. Es importante tener en cuenta que los medios de seguridad están íntimamente relacionados con los avances tecnológicos, es decir, evolucionarán en la medida en que evolucione la tecnología. Para determinar la eficacia, la oponibilidad y la seguridad de las nuevas tecnologías que surjan con este fin será necesario atender el objeto de estos nuevos avances. En otras palabras, cualquier nueva invención tecnológica que tenga como objeto proporcionar seguridad en las transacciones comerciales electrónicas deberá ser considerada un medio de seguridad jurídica. Esta idea tiene su fundamento en la aplicación del principio de equivalencia funcional.

3. Las modalidades y variedades de medios de seguridad son innumerables. Sin embargo, en este trabajo hemos mencionado los medios principales, más comunes y más seguros diseñados hasta el momento. El funcionamiento de las demás modalidades no difiere sustancialmente de las que hemos estudiado.

4. Cada medio de seguridad estudiado pretende solucionar un problema jurídico determinado derivado de la práctica del comercio electrónico. La firma electrónica apunta básicamente a resolver el problema de la integridad y confidencialidad de los mensajes, además de su autoría, y en consecuencia a evitar que sean repudiados. Por su parte, la función de certificación o su elemento material, el certificado digital, soluciona el problema de la identidad de los sujetos que participan en el *e-commerce*. Por último, los medios de pago electrónico permiten la extinción de las obligaciones por medios electrónicos de una manera confiable y oponible a terceras

personas. De esta manera, proporcionan seguridad y certeza jurídica al pago como mecanismo de extinción de obligaciones.

Como vemos, cada medio de seguridad jurídica en el comercio electrónico tiene un objetivo específico. Sin embargo, su eficacia para proporcionar seguridad jurídica en el comercio electrónico está determinada por su funcionamiento en conjunto. Cada uno de estos medios por separado es útil, aunque insuficiente e ineficaz para lograr la tan buscada seguridad en la actividad económica que estamos analizando.

5. Después de estudiar los medios de seguridad jurídica en este capítulo podemos afirmar que la aplicación conjunta de todos ellos forma un sistema de seguridad jurídico. Este sistema permite dotar de seguridad jurídica, de confiabilidad, a las personas que pretendan realizar prácticas de comercio electrónico.

6. Aun cuando la aplicación conjunta de los medios de seguridad estudiados proporciona seguridad jurídica al comercio electrónico, este sistema es falible. Como sucede en el comercio tradicional, existen diversos riesgos en las transacciones comerciales. No nos encontramos ante el remedio absoluto; afirmar lo contrario sería incurrir en una falacia. Sin embargo, concluimos que estos medios de seguridad dan una seguridad y confiabilidad razonables para continuar con la práctica del comercio electrónico y abandonar la idea de descartarlo, pues se trata de un medio de comercio con muchas y mayores ventajas que el comercio tradicional.

7. Es necesario modificar algunas ideas sobre la intervención del Estado en el comercio electrónico, sobre todo en lo que se refiere a medios de seguridad. En efecto, como hemos visto son los medios de seguridad los que permiten la implementación del *e-commerce*. Por este motivo, la participación del Estado en este proceso de implementación debe ser restringida. Es necesario que el Estado delegue al sector privado y a los operadores de comercio electrónico las funciones que brinden confiabilidad a esta actividad. Nos referimos principalmente a dos funciones que tradicionalmente han estado a cargo o supervisión directa del Estado: la función de certificación y la creación de dinero.

8. La función de certificación ha estado tradicionalmente a cargo de los notarios públicos, que ejercen una función pública aunque no dependan del Estado en sentido estricto. En el comercio electrónico esta función está a cargo de las entidades de certificación, que como hemos visto pueden ser personas de derecho público o privado.

El fundamento de esta afirmación es la vocación de universalidad del comercio electrónico. Si la función de certificación estuviera a cargo del Estado, o de personas directamente previamente autorizadas por este, el reconocimiento de esta función en otros países se vería limitada. En efecto, la autorización de la certificación emitida por un Estado no sería reconocida automáticamente, salvo que hubiera un tratado internacional al respecto. Y aunque lo hubiera, todos los países del mundo tendrían que suscribir un tratado similar, que sería inviable en el mediano plazo.

Por este motivo, sostenemos que son los particulares quienes deben ejercer la función de certificación, siguiendo determinados estándares de calidad. El mercado será el encargado de determinar cuáles entidades de certificación son las mejores. De este modo, se obtendrá la confiabilidad del sistema, sin la intervención del Estado.

9. En cuanto a la creación de dinero electrónico, consideramos del mismo modo que en esta actividad no debe intervenir el Estado, al menos no en forma directa. Este hecho se debe a la vocación de universalidad del comercio electrónico, además de que la fluidez y rapidez que lo caracteriza hace necesaria la existencia de medios de pago que sean igualmente rápidos y fluidos. El dinero electrónico es la alternativa para este requerimiento.

Sin embargo, para que el empleo del dinero electrónico sea eficaz es necesario que sea reconocido mundialmente. Por esta razón, aseveramos que el Estado no debe participar en la emisión de dinero electrónico, pues surgiría el mismo inconveniente señalado en el punto anterior: la dificultad de que el dinero electrónico sea reconocido fuera del país donde fue emitido. Sin embargo, consideramos necesaria la participación del Estado de una manera indirecta.

Puede ser mediante la autorización, la supervisión y la fiscalización de las entidades bancarias encargadas de emitir el medio de pago. De este modo, el emisor del dinero sería un ente privado, que podría tener reconocimiento mundial por medio de sucursales, subsidiarias o corresponsales. Detrás de estos entes privados estaría el Estado, fiscalizando su funcionamiento.

CAPÍTULO III
Sistema de seguridad jurídica en el comercio electrónico

1. Introducción

En el capítulo anterior nos hemos dedicado exhaustivamente al desarrollo, descripción y análisis de los medios de seguridad en el comercio electrónico. Como hemos podido apreciar, cada uno de estos medios (firma digital, certificado digital, medios de pago electrónicos y sus complementos tecnológicos) procura resolver uno o más de los problemas relacionados con el comercio electrónico.

Los problemas que surgen con motivo del *e-commerce* están vinculados básicamente al hecho de que el comercio realizado por medio de Internet no permite una proximidad entre los contratantes. Sin esta proximidad, no pueden verificarse una serie de aspectos que les aseguren que su transacción se realizará como tienen previsto, es decir, no podrían tener el margen de previsibilidad que les permita satisfacer sus expectativas. Entre estos aspectos están la identificación de las personas que contratan, la obligatoriedad y la fuerza vinculante de los actos de comercio, la forma de pago, la ley aplicable y los tribunales competentes en caso de disputas.

Como es natural, la proximidad física entre dos contratantes hace muy fácil la tarea de comprobar estos aspectos. Eso no ocurre necesariamente en Internet. Como hemos visto, Internet tiene una

proyección universal que ya se está haciendo realidad. En efecto, en las transacciones por medio de Internet es innecesaria la proximidad física, que facilita la verificación de los elementos que garantizan el éxito de una operación comercial.

En este punto, la tecnología y el Derecho comparten conocimientos que permitirán sortear este obstáculo. Así es como han aparecido los medios de seguridad analizados en el capítulo anterior. Cada uno de estos medios tiene una tarea específica frente a los aspectos que se deben cuidar para que una operación de comercio sea exitosa desde un punto de vista jurídico. En vista de que estos aspectos se traducen en problemas jurídicos, el Derecho debe plantear soluciones.

Para puntualizar cada uno de los problemas y la solución aportada por los medios de seguridad, nos valdremos del siguiente cuadro:

Problema jurídico	Medio de seguridad
Identificación de las partes	Certificado digital. Si bien es cierto que la firma digital asocia la clave pública de una persona con su clave privada, y viceversa, no permite con certeza identificar a la persona, pues la asociación que hace la firma digital mediante la criptografía es matemática, independiente de las características de la persona. Por esta razón, sostenemos que la función de identificación en el comercio electrónico la cumple el certificado digital, que permite identificar a una persona determinada y asociarla con su firma digital.
Integridad de los mensajes	Firma digital. Este medio de seguridad, al emplear la criptografía asimétrica, permite que mensajes e informaciones transmitidos por la red no sean alterados durante su viaje por terceras personas.
Confidencialidad de los mensajes	Firma digital. Del mismo modo, el sistema de criptografía asimétrica empleado por este medio de seguridad evita no solamente que los mensajes sean alterados sino, también, que terceras personas accedan a ellos sin autorización del titular del mensaje.

Repudiación de los mensajes	Firma digital y certificado digital. Como hemos señalado, estos medios permiten la integridad y confidencialidad de los mensajes, así como la identificación de las personas. Por lo tanto, impiden que el autor de un mensaje pretenda no reconocerlo. En efecto, existen medios para determinar tanto la identidad del emisor del mensaje como el contenido del mensaje que transmitió. La combinación de estos medios nos permite evitar el repudio de los mensajes transmitidos por Internet.
Pago de obligaciones	Medios de pago electrónicos. Nos referimos al pago de obligaciones de dar suma de dinero, de acuerdo con la delimitación del estudio de los medios de pago electrónicos realizada para este trabajo. Es indispensable facultar a los sujetos del comercio electrónico para el cumplimiento seguro, desde una perspectiva jurídica, de las obligaciones contraídas. Los medios de pago electrónicos permiten el cumplimiento de estas obligaciones al proporcionar un sistema confiable, eficiente y a la par con la tecnología empleada.
Prueba del pago	Medios de pago electrónicos. La prueba del pago es otra de las preocupaciones al emplear medios electrónicos, pues el tradicional papel sigue muy arraigado en nuestra tradición jurídica. Si bien esta medida de seguridad permite la prueba electrónica de una transacción de pago, será indispensable que cuente con determinadas regulaciones y con reconocimiento jurídico.

De la información que contiene el cuadro anterior podemos concluir que cada medio de seguridad cumple una función determinada. Sin embargo, si son utilizados individualmente, su objetivo de otorgar seguridad jurídica a las operaciones de comercio electrónico sería limitado.

Así, no tendría mucho sentido tener la seguridad de la integridad y confidencialidad de los mensajes (por medio de la firma digital) si no pudiéramos determinar con precisión quién es el autor de los mensajes. En efecto, no podríamos exigir al autor el cumplimiento de las obligaciones contenidas si no tuviéramos certeza de su identidad. Del mismo modo, de nada valdría tener identificado plenamente al autor de un mensaje (por medio del certificado digital) si no pudiéramos garantizar que el mensaje no será alterado en su viaje por la red. Este hecho se debe a que, aunque supiéramos a

quién exigir el cumplimiento de las obligaciones que el mensaje contiene, no podríamos determinar qué obligaciones exigirle, ya que el mensaje podría haber sido alterado en su transmisión y nuevas obligaciones podrían haber sido incorporadas. Por último, de nada nos valdría tener la certeza de la identidad del autor de un mensaje, además de la integridad y confidencialidad del mensaje en sí, si no existiera una forma segura, y oponible a terceros, de extinguir las obligaciones de dar suma de dinero por medios electrónicos (es decir, empleando los medios de pago electrónicos).[1]

Por lo afirmado sostenemos que para garantizar una eficaz seguridad jurídica en el *e-commerce* será necesario que todos estos medios interactúen en un sistema de seguridad integrado. De esta manera, se logrará tener una herramienta de seguridad que asegure la tan buscada seguridad jurídica en el comercio electrónico.

En consecuencia, afirmamos que debe existir un Sistema de Seguridad Jurídica en el Comercio Electrónico (en adelante, SSJ) que esté integrado por los diversos medios de seguridad estudiados en el capítulo anterior y regulado por determinados principios que determinen su funcionamiento. A continuación desarrollaremos estas ideas para describir el funcionamiento de este sistema de seguridad.

2. DEFINICIÓN

No hemos encontrado en la bibliografía consultada una definición de sistema de seguridad jurídica de acuerdo con los términos expresados. Nosotros proponemos la siguiente definición:

El sistema de seguridad jurídica en el comercio electrónico es el conjunto de medios de seguridad electrónicos que interactúan en forma ordenada, de acuerdo con lo establecido por los principios de seguridad jurídica en el comercio electrónico. Su objetivo es procurar

---

[1] Nos referimos, únicamente, a las obligaciones de dar suma de dinero, ya que en el capítulo anterior, en la parte relativa a medios de pago electrónicos, delimitamos este estudio a los medios de pago electrónicos como medios para extinguir obligaciones de dar suma de dinero.

la seguridad jurídica en las diversas operaciones de comercio electrónico que se pueden realizar por medio de redes abiertas.

Precisemos, a continuación, algunos conceptos empleados en esta definición.

2.1. Medios de seguridad electrónicos

Por medios de seguridad electrónicos debemos entender los avances tecnológicos que facilitan la obtención de seguridad jurídica en las operaciones de *e-commerce*.

No hemos mencionado en nuestra definición los medios de seguridad jurídica estudiados en el capítulo II, pues pretendemos que nuestra definición tenga un carácter abierto y no cerrado a determinados medios.

De este modo, pretendemos que la definición se adapte a los constantes cambios tecnológicos, pues, como hemos visto en anteriores oportunidades, la tecnología avanza con mucho más rapidez que el Derecho. Así, toda definición está amenazada con quedar obsoleta prácticamente desde su nacimiento.

Para que sea considerado como tal, bastará entonces con que el SSJ esté integrado por cualquier medio de seguridad que permita cumplir con las funciones que más adelante estudiaremos.

2.2. Principios de seguridad jurídica en el comercio electrónico

Como hemos visto en el capítulo anterior, la seguridad jurídica en materia de comercio electrónico tiene un matiz diferente y particular, al tratarse de una realidad mucho más dinámica y evolutiva que otras ramas del Derecho y del comercio.

Lógicamente, el SSJ deberá estar regulado por ciertos principios aplicables exclusivamente para él mismo. Este requisito no supone que consideremos el comercio electrónico y su sistema de seguridad como realidades distintas y completamente diferentes a otras ramas del Derecho y del comercio, sino que requieren de determinadas

herramientas especiales debido a sus propias características. Por este motivo, requerirá de principios orientadores propios.

2.3. Seguridad jurídica

La seguridad jurídica en el SSJ tiene como fin asegurar que los sujetos que participan en una operación de comercio electrónico tengan certeza en la consecución de los fines que persigan al llevar a cabo una operación de *e-commerce*.

En este contexto, entendemos «certeza» como la capacidad de determinar y garantizar razonablemente lo siguiente:

- *La identidad de los sujetos del comercio electrónico*. Al poder determinar la identidad de las personas que contraen obligaciones, se logra identificar al sujeto que estará obligado a la ejecución de determinada prestación. De este modo, se le podrá exigir el cumplimiento de sus obligaciones.
- *La integridad y confidencialidad de los mensajes transmitidos por medio de la red*. Una vez identificados los sujetos a los que se podrá exigir el cumplimiento de ciertas obligaciones, y estando garantizada la integridad de los mensajes, así como la confidencialidad, podremos determinar qué exigir a estos sujetos. De este modo, los mismos sujetos tendrán la garantía de que se les exigirá únicamente el pago de las obligaciones que desearon contraer y no otras distintas.
- *La eficacia del pago realizado por medios electrónicos*. Así como los sujetos tendrán interés en contraer determinadas obligaciones para que les sean exigidas, del mismo modo tendrán interés en tener la certeza de que estas obligaciones tendrán un efecto extintorio mediante los medios de pago electrónicos. El razonamiento es el siguiente: de qué vale tener certeza al contraer determinadas obligaciones, si no tendré certeza de que estas obligaciones se extinguirán en un medio de pago electrónico.
- *Un medio de prueba*. El medio de prueba es un elemento de certeza complementario para nuestro SSJ. Se trata de una función agregada de los medios de seguridad, que incluyen el mérito

probatorio y, por ende, la posibilidad de servir de prueba de los diversos actos jurídicos que se realicen en Internet.

Debemos precisar que la seguridad en nuestro SSJ se refiere primordialmente al ámbito de derecho sustantivo. Su fin es lograr la certeza de la existencia de actos jurídicos válidos y oponibles frente a terceras personas. No está diseñado para ser aplicado en un plano de derecho adjetivo o procesal.

Lo anterior no significa que consideremos que se deba mantener así, ni que su funcionamiento sea perfecto sin tomar en consideración los aspectos adjetivos. Por el contrario, somos de la opinión de que debe ser complementado por un sistema que permita la ejecución y la exigencia efectiva de las obligaciones que se contraigan en los medios electrónicos. Aplicando el razonamiento empleado al momento de evaluar individualmente los medios de seguridad, ¿de qué valdría tener un sistema de seguridad jurídico que permitiera tener certeza respecto de los contratantes, las obligaciones contraídas y la efectividad de los medios de pago, si no se existiera un mecanismo jurídico que garantizara la ejecución de estas obligaciones, en caso de su incumplimiento?

Los aspectos adjetivos no son el objeto de estudio principal de este trabajo. Por esta razón, no precisamos ni ahondamos en los temas de connotación adjetiva. Sin embargo, no por ello dejamos de señalar que los aspectos de orden adjetivo son muy importantes para lograr la seguridad jurídica en el comercio electrónico.

Podemos decir entonces que la seguridad jurídica en el comercio electrónico puede estar agrupada en dos categorías: la seguridad jurídica en un plano sustantivo y la seguridad jurídica en un plano adjetivo. El objeto de este estudio es la primera categoría.

3. CARACTERÍSTICAS

Las principales características del SSJ son las siguientes:

- Tiene como función dotar al comercio electrónico de un nivel de seguridad jurídica aceptable y razonable que permita su desarrollo

y práctica. Decimos seguridad aceptable porque ningún sistema de seguridad será completamente seguro en un cien por ciento, tal como afirma Maltese: «Efectuar compras seguras en un cien por ciento no existe en la actualidad, al igual que en la vida real. Pero el avance científico nos va permitiendo aproximar cada vez más al concepto óptimo de seguridad».[2]

- Está compuesto por los siguientes elementos: los sujetos del comercio electrónico, los prestadores de servicios de certificación, las entidades financieras y los medios tecnológicos pertinentes (*hardware*: computadoras con suficiente capacidad, y *software*: programas empleados para la firma digital, la función Hash, la ejecución de la certificación, las pasarelas de pago y la generación de dinero electrónico, entre otros programas).
- Está íntimamente vinculado al desarrollo tecnológico, ya que, como hemos visto, está compuesto por medios de seguridad jurídica electrónicos cuya base es fundamentalmente tecnológica.
- Aquí se pone en evidencia la íntima vinculación del Derecho con la tecnología, pues la seguridad jurídica de las operaciones comerciales dependerá de los avances tecnológicos. Los diversos medios de seguridad que compongan este sistema podrán cambiar a medida que la tecnología cambie y evolucione.
- Está regulado por determinados principios que le son exclusivamente aplicables y adicionalmente por los principios que regulan las operaciones de comercio tradicionales.
- Su eficacia jurídica como sistema no se encuentra en relación de dependencia con el Estado. En efecto, el funcionamiento de cada uno de sus elementos no tiene una dependencia directa del Estado, cuya participación proponemos debe ser indirecta.
- Es un sistema de seguridad jurídica que tiene una vocación de universalidad, es decir, podrá emplearse en cualquier parte del mundo, sin fronteras legales ni físicas.

---

[2] MALTESE, Mariano. El pago electrónico en Argentina». En <http://www.vlex.ar/cn/Derecho_Inform@tico/12>.

- Se trata de un sistema flexible, abierto a los cambios tecnológicos y comerciales, y de fácil adaptación. Por lo tanto, tiene vocación de permanencia.

4. FUNCIONES DEL SISTEMA DE SEGURIDAD JURÍDICA EN EL COMERCIO ELECTRÓNICO

La única función del SSJ es dotar al comercio electrónico de una seguridad razonable para su práctica. Para lograrlo requiere cumplir con las siguientes funciones:

4.1. Función de identificación de los sujetos del comercio electrónico

Al lograr la identificación de los sujetos del comercio electrónico se puede conocer a la persona que se obliga a determinada prestación. Además, se hace posible exigirle el cumplimiento de la prestación en el momento oportuno.

Del mismo modo, permite verificar las cualidades de las personas con las que se contrata. Así se podrá formar una voluntad de contratar de acuerdo con los requerimientos de cada persona, evitando casos de fraude o suplantación, entre otros hechos dolosos.

También permite verificar las capacidades legales de las personas con las que se contrata. Por ejemplo, determinar la capacidad de los contratantes; la adecuada representación, de ser el caso; y el domicilio de los sujetos, entre otros datos de carácter legal.

La función de identificación en el SSJ se logra actualmente con las entidades de certificación y con el certificado digital, que al reunir determinadas características están en condiciones de garantizar la identidad de los titulares de firmas digitales.

4.2. Función de identificación de los mensajes transmitidos

La función de identidad de los mensajes tiene por objeto dotar de identidad a los mensajes electrónicos transmitidos en la red. La

identidad de un mensaje está en función de la determinación de su autor, de su contenido y de su destinatario.

La efectiva determinación de la autoría de un mensaje y la integridad de su contenido, sin la posibilidad de que agentes distintos del remitente de un mensaje puedan modificar la información que contenga, resuelve el problema de la integridad de los mensajes que se transmiten por la red.

La posibilidad de garantizar que el contenido de un mensaje sea revelado solo al destinatario y, por lo tanto, conocido únicamente por él, sin que terceros no autorizados puedan acceder a esta información, resuelve el problema de la confidencialidad de los mensajes.

La función de identificación de los mensajes y, por ende, la solución de los problemas de integridad y confidencialidad en el SSJ se logran actualmente con la firma digital, mediante el empleo del sistema de criptografía asimétrica.

4.3. Función de vinculación de los sujetos

La función de vinculación tiene por objetivo solucionar el problema de la repudiación de los mensajes transmitidos en Internet. En efecto, permite que el acreedor en una operación de comercio electrónico exija a su deudor el cumplimiento de las obligaciones contraídas e imposibilita al deudor negar la autoría del mensaje con el cual contrajo su obligación, además de los términos en que la contrajo.

Para poder exigir una obligación a una persona debemos, en primer lugar, identificarla, ya que no se puede exigir una obligación a una persona que no la contrajo. En segundo lugar, debemos identificar los términos en los que esta persona se obligó para exigir la prestación. En efecto, no se puede exigir a una persona el cumplimiento de las obligaciones que contrajo en términos distintos a los pactados, de acuerdo con lo establecido en el artículo 1361 del Código Civil.

Por lo tanto, la función de vinculación de sujetos se lleva a cabo identificando plenamente al deudor de la obligación pendiente de pago. Esto se logra con la función de identificación de los sujetos (por medio del certificado digital). En segundo lugar, se identifica el

mensaje que contiene la obligación contraída, y eso se logra con la función de identificación de los mensajes (por medio de la firma digital).

En conclusión, podemos ver que la función de vinculación de sujetos se lleva a cabo con la aplicación combinada de la función de identificación de los sujetos y la función de identificación de los mensajes.

4.4. Función de oponibilidad del pago electrónico

Con esta función se busca solucionar el problema de la eficacia del pago efectuado por medios de pago electrónicos para extinguir obligaciones.

En el SSJ, esta función es cumplida con los medios de pago electrónicos, y todas sus variedades, las que han sido desarrolladas en el capítulo anterior. Como hemos indicado, los medios de pago electrónicos son medios que permiten extinguir obligaciones. Esta posibilidad permite que se oponga este efecto extintorio tanto al acreedor como a terceras personas.

Debemos nuevamente aclarar que la función de oponibilidad del pago se refiere al pago de obligaciones de dar suma de dinero, a las que en este trabajo se hace referencia.

4.5. Función probatoria

Esta función, como hemos visto en este capítulo, es una accesoria a las antes mencionadas. En efecto, no tiene su correlato en un medio de seguridad específico, sino que se encuentra en cada uno de los medios de seguridad.

Por ejemplo, en la función de identificación de los mensajes, que emplea la firma digital, la función probatoria del sistema se cumplirá con la firma misma, con el algoritmo matemático que resulte de la aplicación de la función Hash a la firma digital y al mensaje transmitido. En el caso de la función de identificación de los sujetos, empleando el certificado digital, la función probatoria será cumplida con la emisión del certificado digital. Por último, en la

función de oponibilidad del pago, los comprobantes de pago —electrónicos o físicos— cumplirán con la función probatoria.

Como podemos apreciar, esta función se encuentra en cada una de las funciones. El tema a tratar en cuanto a la función probatoria y a la prueba en sí es el soporte en el que se almacenan el certificado digital, la firma digital o el comprobante electrónico emitido al emplear un medio de pago electrónico determinado.

¿Cuál será el soporte válido para dotar de carácter probatorio a los medios de prueba indicados? ¿El ordenador que los contiene, un disco compacto, un disquete o la impresión de los medios de prueba?

Consideramos que fijar el mérito probatorio únicamente en base a la determinación de un soporte físico es insuficiente. Será necesario que se permita su comprobación con la ejecución del protocolo o del proceso que dio origen al medio electrónico de prueba ofrecido. La manipulación o imitación de la información relacionada con una prueba contenida en un soporte físico será evidente al constatar el origen de la información, recreando el proceso que le dio origen.

Se entiende, entonces, que este sistema de verificación implica que cada una de las operaciones de comercio electrónico deberá ser registrada para que sea posible recrear —en un momento determinado y con las autorizaciones debidas— la ejecución de las operaciones realizadas que originaron el documento electrónico y así determinar su correcta ejecución.

4.6. Función de intermediación

Nuestro ordenamiento jurídico ha contemplado la posibilidad del registro de las operaciones de comercio electrónico en el Reglamento de la Ley de Firmas y Certificados Digitales, decreto supremo 019-2002-JUS,[3] al establecer en su artículo 4 la función de intermediación digital (FI). Esta es definida en los siguientes términos:

[3] Publicado en el diario oficial *El Peruano* el 18 de mayo de 2002.

> Procedimiento facultativo al que se accede expresa y voluntariamente, por el cual, en la transmisión de un mensaje de datos o documento por vía electrónica, con firma digital, interviene un Tercero Neutral que cumple con lo establecido por el Decreto Legislativo n.° 681 con el fin de grabar, almacenar y conservar los contenidos de mensajes de datos y documentos en un micro archivo; y certificar respecto a ellos, a solicitud de los interesados o de las autoridades competentes, los datos sobre su envío, fecha y hora de recepción por el destinatario; identificación del emisor; y el contenido, autenticidad y no alteración de los textos; y cualquier otro legalmente posible. Pueden prestar este servicio aquellas personas que cumplen con las normas establecidas en el Decreto Legislativo N° 681[4] y sus normas modificatorias y reglamentarias.

La FI parte de la siguiente premisa: cuando se lleva a cabo una transacción electrónica se generan una serie de documentos electrónicos que son prueba de la ejecución de la transacción. Por ejemplo, en una compraventa electrónica podrían generarse los siguientes: la cotización del proveedor, la orden de pedido del consumidor y la orden de transferencia electrónica de fondos del consumidor a su banco para el pago, así como las constancias de recibo de los documentos. Todos ellos son prueba de la transacción ejecutada.

En consecuencia, al generarse documentos electrónicos que sirven de medios probatorios de las transacciones ejecutadas, la función de intermediación permite otorgar un mérito probatorio a los documentos, almacenándolos y garantizando su reproducción fidedigna. De este modo, la función de intermediación complementa la función probatoria del SSJ, cuyas características son las siguientes:

4.6.1. Función facultativa

No será obligatorio que los sujetos del comercio electrónico se sometan a la función de intermediación. Nos parece adecuado, pues

---

[4] Decreto legislativo 681. Dicta normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información, tanto respecto al elaborado en forma convencional cuanto al producido por procedimientos informáticos en computadoras. Publicado en el diario oficial *El Peruano* el 14 de octubre de 1991.

serán los propios sujetos quienes decidan someterse o no a esta función, de acuerdo con sus requerimientos de seguridad.

Como es evidente, no todas las transacciones por medios electrónicos requerirán de los mismos niveles de seguridad; en consecuencia, no siempre será necesaria la ejecución de la función de intermediación. Si fuera obligatoria podrían incrementarse inútilmente los costos de ciertas transacciones que no requieren de niveles de seguridad altos. Este hecho podría desmotivar el empleo de medios electrónicos para realizar operaciones comerciales de bajos montos e, incluso, podría tener implicancias discriminatorias.

4.6.2. Tercero neutral

El tercero neutral es el elemento subjetivo de la función de intermediación, pues es quien tiene a su cargo su ejecución.

El citado artículo 4 del Reglamento de la Ley de Firmas y Certificados Digitales define al tercero neutral en los términos siguientes:

> Persona facultada de conformidad con el Decreto Legislativo n.° 681 y sus normas modificatorias y reglamentarias, para grabar, almacenar o conservar, cuando corresponda los contenidos de mensajes transmitidos por vía electrónica. De acuerdo con lo dispuesto en las normas citadas, el Notario o Fedatario, con certificado de Idoneidad Técnica expide copia certificada de los mensajes de datos e insertos, con valor probatorio, certificando quién es el titular de la firma digital que se identifica con el mensaje de datos o documento, cuándo fue expedido y recibido, la no alteración de los textos y cualquier otro dato legalmente posible.

Según esta definición, el tercero neutral, como ocurre con las entidades de certificación, cumple una función pública que consiste en dar fe de la autenticidad de los documentos electrónicos archivados que se generen a partir de una operación de comercio electrónico. Del mismo modo, debe dar fe de las copias certificadas que se obtengan, que pueden ser empleadas como medios probatorios en procesos judiciales.

El tercero neutral estará facultado para expedir copias certificadas de los mensajes de datos y de sus insertos con pleno valor probatorio. En cierto sentido, podría considerarse al tercero neutral como

un notario público o fedatario electrónico, pues cumple una función similar que consiste en dar fe de la autenticidad de los documentos electrónicos generados en una operación de comercio electrónico.

4.6.3. Objetivos

La función de intermediación tiene dos objetivos: el registro y la publicidad.

El registro es la grabación, almacenamiento y conservación de los contenidos de mensajes de datos y documentos en un microarchivo. Estas operaciones garantizan que el contenido de los mensajes no sea desconocido por los autores, además de permitir la existencia de un medio probatorio idóneo y con plenos efectos legales.

La publicidad permite el conocimiento del contenido de los mensajes de datos registrados por medio de copias certificadas, que tienen igual valor que los mensajes registrados. Con la publicidad será posible conocer los datos de envío de un mensaje, la fecha y hora de recepción por el destinatario, la identificación del emisor y el contenido y la autenticidad de los textos, además de saber que no han sido alterados.

4.6.4. Función pública

Tomando en cuenta los objetivos de la función de intermediación —cuyo fin principal es dar fe de los mensajes y documentos generados en operaciones de comercio electrónico— consideramos que es una función pública, con las prerrogativas legales que ello implica.

Dicha naturaleza supone la necesidad de contar con mecanismos legales de fiscalización para garantizar la idoneidad técnica y moral, además de capacitar a quienes tengan a su cargo la ejecución de la función de intermediación.

Consideramos necesario, antes de terminar con el análisis de la FI, hacer una precisión. Como hemos señalado, esta función es ejercida por los terceros neutrales, a quienes podría considerarse unos de los sujetos que forman parte del SSJ o, en todo caso, parte de la estructura misma del sistema. Sin embargo, consideramos que no sería correcto, pues la FI tiene un carácter accesorio. En

efecto, no se podría desproteger jurídicamente las transacciones en las cuales no se ejecute esta función. Lo contrario llevaría a concluir que el carácter de medios de seguridad jurídica de la firma y del certificado digital, así como los medios de pago electrónicos, dependen de la función de intermediación. Este hecho desvirtuaría la presencia de los medios en el SSJ propuesto.

En el comercio electrónico, la FI es una opción que proporciona una mayor seguridad jurídica a las operaciones comerciales, dando mayor soporte a la función probatoria del SSJ. Por esta razón, apostamos por una incorporación voluntaria de esta función, aceptada por acuerdo expreso de las partes.

5. Funcionamiento del sistema de seguridad jurídica en el comercio electrónico

5.1. Requisitos para el funcionamiento del sistema de seguridad jurídica en el comercio electrónico

Los requisitos para el empleo del SSJ son los siguientes:

- Todas las partes que integren el SSJ deberán tener una firma y certificado digital.
- Los sujetos participantes deben contar con los medios tecnológicos adecuados.
- Las entidades prestadoras de servicios de certificación deben reunir los estándares adecuados para la prestación de estos servicios.
- Las entidades financieras que presten los servicios de emisión de dinero electrónico deben contar con la infraestructura y con la capacitación necesarias.
- El Estado debe reconocer la naturaleza de las operaciones de comercio electrónico para aceptar su participación indirecta en determinadas actividades vinculadas con esta modalidad de comercio.[5]

[5] Entre estas actividades están la función de certificación y la emisión de dinero electrónico.

- Debe existir una entidad —o entidades— con reconocimiento internacional, capaz de solucionar conflictos derivados de la ejecución de operaciones de comercio electrónico.

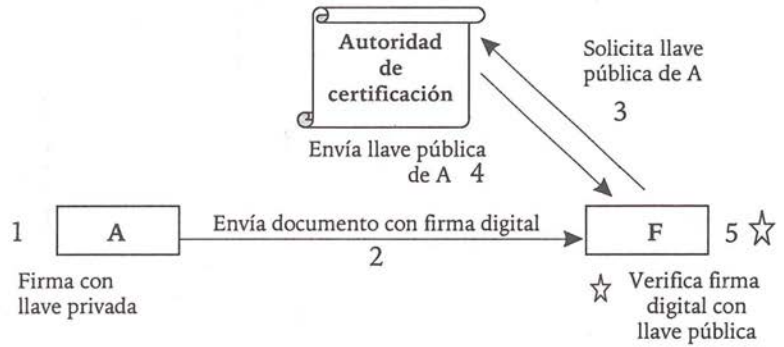
5.2. Funcionamiento del sistema de seguridad jurídica en el comercio electrónico

La operatividad del SSJ está en función a la acción combinada de los medios de seguridad estudiados. En una operación simple de comercio electrónico, en la que se adquiera un bien determinado y se cancele el precio en un mismo instante, se combina el funcionamiento de los tres medios de seguridad estudiados. Sin embargo, para explicar su funcionamiento combinado, lo haremos por separado.

5.2.1. Envío de mensaje firmado digitalmente

Explicaremos este proceso con el siguiente gráfico:

Envío de mensaje firmado digitalmente



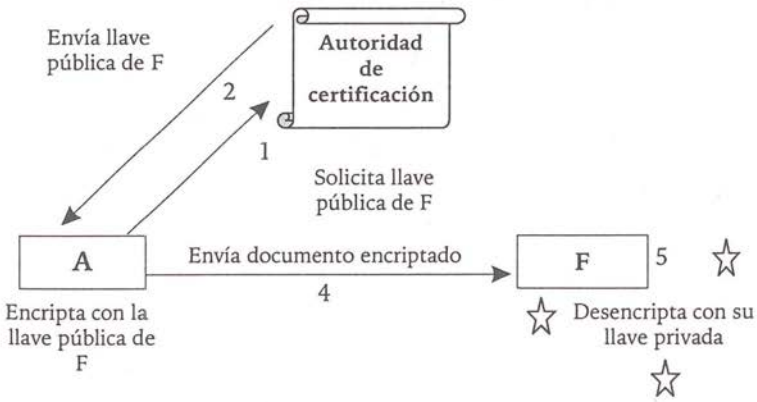
1. A firma digitalmente el mensaje con su clave privada.
2. Envía el mensaje firmado a F por la red.
3. Una vez recibido el mensaje, F solicita la clave pública de A para poder descifrar el mensaje.
4. La entidad de certificación envía la clave pública a F.
5. Una vez recibida la clave pública de A, F descifra el mensaje y tiene acceso a su contenido.

En este caso, A simplemente envía un mensaje que ha firmado digitalmente. Esta operación tiene por objetivo asegurar la identificación del autor del mensaje, aunque parcialmente, puesto que únicamente con la clave pública de A descifrará el mensaje cifrado con la clave privada de A. Sin embargo no se garantiza que se trate del titular de la firma empleada. Al mismo tiempo, tiene el segundo objetivo de garantizar que el mensaje no haya sido alterado o modificado en su tránsito por la red. En este caso, es imposible garantizar la identificación del autor y la imposibilidad de repudiación del mensaje.

5.2.2. Envío de mensaje cifrado

Con el siguiente gráfico explicaremos el proceso del envío de los mensajes cifrados:

Envío de mensaje encriptado



1. A, quien quiere enviar un mensaje a F, solicita a la entidad de certificación la clave pública de F.
2. La entidad de certificación envía a A la clave pública de F.
3. A cifra el mensaje que enviará a F con la clave pública del último.
4. A envía el mensaje cifrado a F por medio de la red.
5. F descifra —con su clave privada— el mensaje que le ha sido enviado.

Como se puede ver, el envío de mensajes de esta forma únicamente garantiza la confidencialidad e integridad del mensaje. En efecto, solo el mensaje que F ha recibido podrá ser descifrado con su clave privada, al haber sido cifrado con su clave pública. Sin embargo, este empleo parcial de la firma digital no permite garantizar la autoría del mensaje, ya que no se tiene certeza de que la clave pública de A ha sido empleada por él mismo.

5.2.3. Envío de mensaje autenticado

Llamamos «mensaje autenticado» al mensaje en el que está garantizada, en primer lugar, la identidad del autor por medio del certificado digital y, en segundo lugar, la integridad y confidencialidad de los mensajes, con el empleo de la firma digital. De este modo, se ejecuta la función de identificación de los sujetos y la de los mensajes transmitidos.

El envío de un mensaje autenticado por Internet implica necesariamente que los diversos remitentes y destinatarios tengan una firma y un certificado digitales.

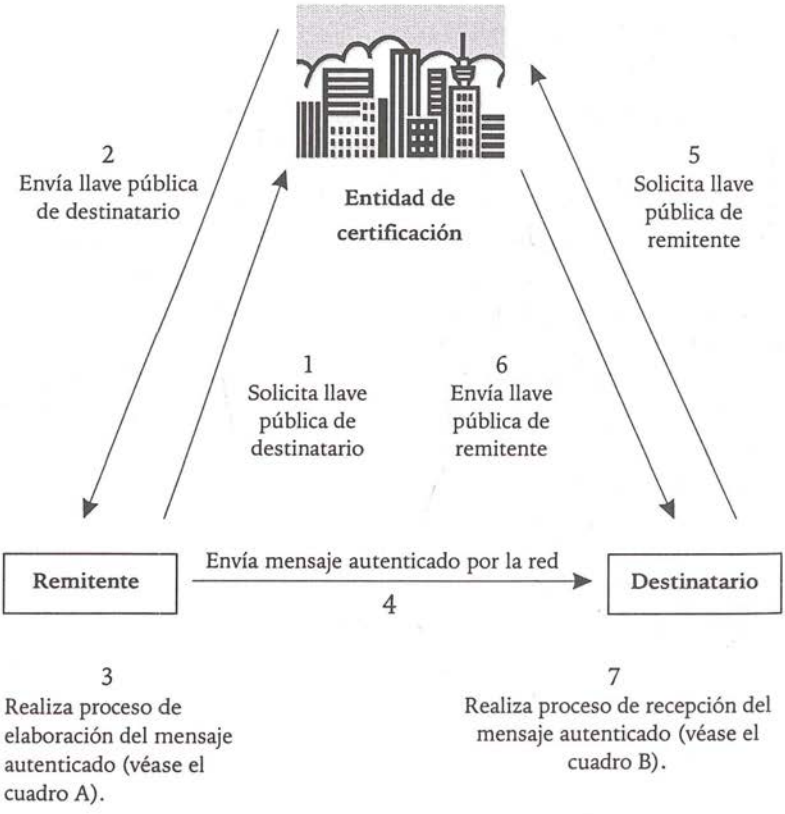
A continuación explicaremos el proceso de envío de un mensaje autenticado, empleando el gráfico de la página siguiente.

El proceso se inicia cuando el remitente de un mensaje se comunica con una entidad de certificación determinada para que le remita la clave privada del destinatario del mensaje. Este paso tiene como objetivo enviar un mensaje con la seguridad de que se mantendrá íntegro y confidencial en su travesía por la red, aplicando así la función de identificación de los mensajes.

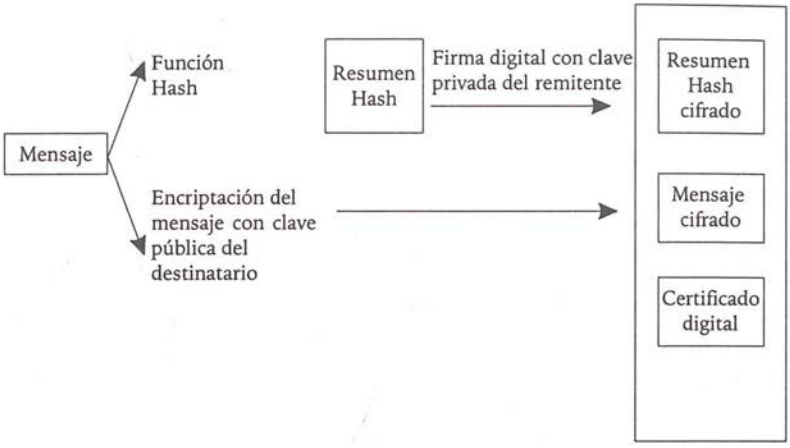
En la segunda etapa, la entidad de certificación contactada por el remitente envía la clave pública del destinatario por la red. La entidad de certificación enviará la clave pública firmada digitalmente para lograr la integridad y confidencialidad de la misma. El mensaje que contiene la clave pública del destinatario será descifrado con la clave pública de la entidad de certificación.

Como vemos, la entidad de certificación cumplirá la función de publicidad de las claves públicas de sus clientes y, del mismo modo, verificará la identidad del destinatario.

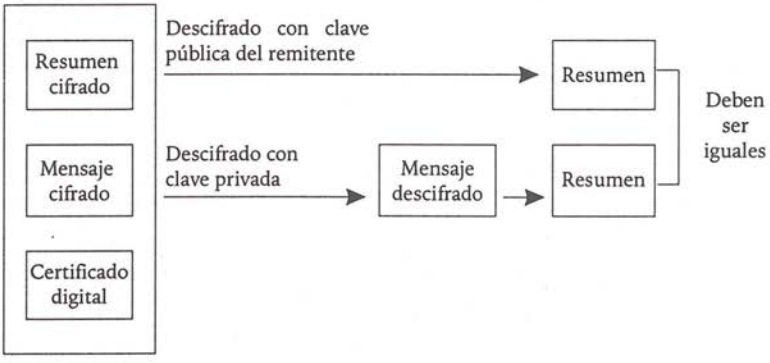
Proceso de envío de mensaje autenticado



Cuadro A
Proceso de envío de un mensaje firmado digitalmente y que contiene un certificado digital



Cuadro B
Proceso de recepción de un mensaje firmado digitalmente y que contiene un certificado digital



En la tercera etapa, el remitente elabora el mensaje autenticado, proceso que podemos apreciar en el cuadro A de la página anterior, que a continuación explicamos.

En el proceso de elaboración de un mensaje autenticado, el remitente aplica a su mensaje original la función Hash, con lo que obtiene un resumen Hash. Este a su vez es cifrado con su clave privada. Del mismo modo, cifra con su clave privada el mensaje original.

Tanto el resumen Hash cifrado como el mensaje original cifrado son incluidos en el mensaje que se enviará, incorporando adicionalmente el certificado digital del remitente emitido por su propia entidad de certificación. De este modo, se obtiene el mensaje autenticado que contiene un resumen Hash del mensaje original cifrado, el mensaje original cifrado y el certificado digital del remitente.

El mensaje autenticado garantiza, en primer lugar, la integridad y confidencialidad del mensaje al emplear la firma digital (y con ella la función Hash). En segundo lugar, permite la identificación de las partes, al emplear el certificado digital. De este modo, se cumple plenamente con las funciones del SSJ de identificación del mensaje y de su autor.

La cuarta etapa consiste en el envío del mensaje autenticado por medio de Internet al destinatario.

En la quinta etapa, luego de recibir el mensaje autenticado, el destinatario solicita su clave pública a la entidad de certificación del remitente para descifrar el mensaje original y el resumen Hash del mensaje original y comprobar la integridad del mensaje. El destinatario sabrá con seguridad a qué entidad de certificación dirigirse, pues en el certificado digital que acompaña al mensaje autenticado estarán los datos de la entidad.

En la sexta etapa, la entidad de certificación del remitente envía al destinatario la clave pública del remitente. Además de practicar la función de publicidad de claves, la entidad realiza la función de identificación de las partes al confirmar la identidad del remitente.

En la séptima etapa, el destinatario recibe el mensaje autenticado, graficado en el cuadro B de la página 239 y que explicamos a continuación:

- Una vez recibida la clave pública del remitente, el destinatario procede a descifrar el resumen cifrado y obtiene el resumen descifrado. De igual manera, descifra el mensaje cifrado y obtiene el mensaje original al que le aplicará la misma función Hash que le aplicó el remitente.
- Así se obtendrán dos resúmenes Hash descifrados: el resumen generado por el remitente y el resumen generado por el destinatario. Deberán ser idénticos para verificar la integridad del mensaje original.
- Del mismo modo, en esta etapa el destinatario será capaz de verificar la identidad del remitente al tener a la vista su certificado digital.

Debemos señalar que el sistema de envío de mensajes autenticados se aplica a cualquiera de las etapas del comercio electrónico, ya sea localización de las partes, contratación electrónica o ejecución.

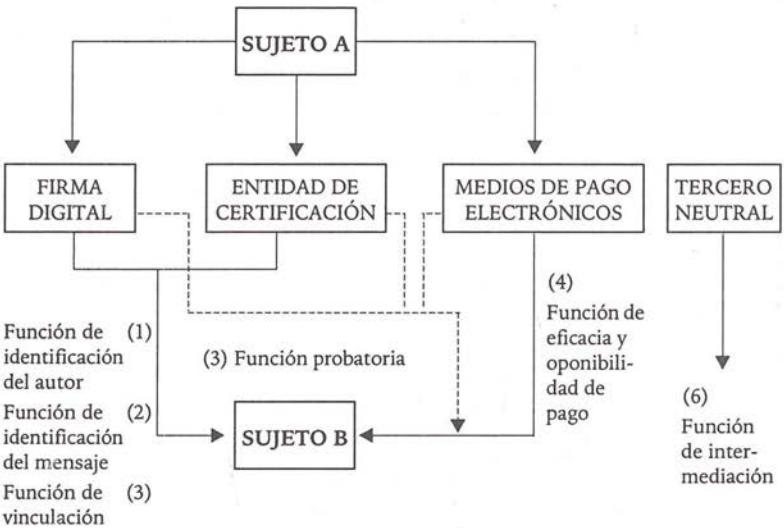
Para la fase de ejecución o conclusión de contratos —en especial en lo referente al pago por medios electrónicos—, el SSJ reúne a la firma y el certificado digitales con los medios de pago electrónicos, para aplicar la función de oponibilidad del pago. De esta manera, los medios de pago electrónicos garantizan la generación confiable de los medios que permiten la extinción de obligaciones para que el pago efectuado sea oponible al acreedor y a terceras personas. El sistema de mensajes autenticados, por su parte, permite que los medios de pago generados en forma confiable sean transmitidos por la red también de una manera confiable.

Como podemos apreciar, se complementan los medios de seguridad jurídica del SSJ para lograr la efectividad de la función de oponibilidad del pago realizado en medios electrónicos.

5.2.4. Funcionamiento del sistema de seguridad jurídica en el comercio electrónico

El empleo combinado de los envíos de mensajes estudiados describe el funcionamiento del SSJ, que describimos con el siguiente gráfico.

Funcionamiento del sistema de seguridad jurídica en el comercio electrónico



El gráfico muestra el funcionamiento en conjunto del SSJ. Asimismo, muestra la forma en que dos sujetos se pueden vincular jurídicamente al realizar cualquier operación de *e-commerce*.

A modo de ejemplo, supongamos que el sujeto A inicia la operación de comercio (por ello, las flechas parten del sujeto A y se dirigen al sujeto B). Para lograrlo emplea el sistema de mensaje autenticado (usando la firma digital y el certificado digital emitido por su entidad de certificación) y envía un mensaje realizando una oferta de compra determinada. De este modo, el sujeto A está dirigiendo una oferta al sujeto B, con los alcances establecidos en el artículo 1382 del Código Civil.[6]

[6] Artículo 1382 del Código Civil: «La oferta obliga al oferente, si lo contrario no resulta de los términos de ella, de la naturaleza de la operación o de las circunstancias del caso».

El sujeto B, usando el mismo sistema de mensaje autenticado, envía su aceptación de la oferta formulada, cuyo efecto es una obligación en los términos establecidos en el artículo 1373 del Código Civil.[7]

En una segunda etapa de ejecución de las obligaciones contraídas, el sujeto A se vale de los medios de pago electrónicos para lograr el efecto extintorio de las obligaciones asumidas de dar suma de dinero. Así, se logran los efectos jurídicos del pago contemplados en el artículo 1220 del Código Civil.[8]

Como se puede apreciar en el gráfico, el recuadro de la firma digital y el recuadro de la entidad de certificación están finalmente unidos por una línea. Esta ilustración indica que estos dos medios combinados cumplen la función de identificación del autor y del mensaje, además de la función de vinculación. De este modo, con su aplicación conjunta se garantiza la formación de un acto jurídico válido y eficaz, que puede ser cualquier acto de comercio, dentro de cualquiera de las etapas del comercio electrónico.

En el mismo gráfico se encuentran, en un recuadro, los medios de pago electrónicos, que cumplen la función de eficacia y oponibilidad del pago. Podemos ver que, en cualquier obligación contraída en la que sea posible pagar con medios electrónicos, el empleo de estos medios de pago garantizará la eficacia y la oponibilidad del pago.

Las líneas punteadas muestran el cumplimiento de la función de prueba del SSJ que, como hemos señalado, se cumple en forma complementaria por cada medio de seguridad jurídica. Además, puede ser complementada con la función de intermediación si así lo acuerdan los sujetos participantes en una operación de comercio electrónico.

En la función de intermediación no se encuentra unida al SSJ, pues no forma parte necesariamente del SSJ, siendo esta de carácter

---

[7] Artículo 1373 del Código Civil: «El contrato queda perfeccionado en el momento y en el lugar en que la aceptación es conocida por el oferente».

[8] Artículo 1220 del Código Civil: «Se entiende efectuado el pago solo cuando se ha ejecutado íntegramente la prestación».

facultativo, aunque nosotros somos de la opinión que es una función de carácter indispensable.

El sentido del gráfico en el ejemplo propuesto va del sujeto A hacia el sujeto B. Sin embargo, el sentido puede ser inverso y puede representar cualquier tipo de operación de comercio electrónico. Del mismo modo, no se trata de un gráfico cerrado a la participación de agentes adicionales: pueden intervenir otros sujetos o entidades (como las financieras o los terceros neutrales), aunque su participación será accesoria y voluntaria, como hemos señalado.

5.3. Modelo de transacción de comercio electrónico con el sistema del mensaje autenticado

A manera de ejemplo, a continuación describiremos cómo se emplea el sistema del mensaje autenticado en una operación completa de *e-commerce*.[9]

En este modelo se ejemplifica una operación de compraventa de mercadería. Esta operación se inicia con el envío de una oferta de venta de un comerciante a un potencial consumidor. Intervienen una entidad de certificación y los bancos de las partes al efectuarse el pago con dinero electrónico.

La operación consta de 21 fases divididas en las cuatro siguientes etapas:

5.3.1. Etapa de contratación electrónica entre el comerciante y el consumidor. Fases 1 a 8

Fase 1: el comerciante (en adelante, *comercio*) que ofrece el producto a su potencial consumidor (en adelante, *cliente*) solicita a la entidad de certificación del *cliente* su clave pública para remitirle su oferta de venta.

Fase 2: la entidad de certificación envía al *comercio* la clave pública del *cliente*.

---

[9] Véase el cuadro de la página 238.

Fase 3: el *comercio* elabora el mensaje autenticado que contiene su oferta de venta.[10]

Fase 4: el *comercio* envía por la red el mensaje autenticado al *cliente*.

Fase 5: el *cliente* recibe el mensaje autenticado y solicita a la entidad de certificación la clave pública del *comercio* para recibir el mensaje autenticado.

Fase 6: la entidad de certificación remite al *cliente* la clave pública del *comercio*.

Fase 7: el *cliente* recibe el mensaje autenticado.[11]

Fase 8: el *cliente* envía por Internet la aceptación de la oferta formulada por el *comercio*, para lo cual elabora el mensaje autenticado que contiene su aceptación. Una vez que el *comercio* haya recibido el mensaje autenticado, llevará cabo el proceso de recepción del mensaje. En esta etapa no será necesaria la solicitud de las claves públicas, pues ya son de conocimiento de ambas partes.

5.3.2. Etapa de contratación entre el consumidor y su banco. Fases 9 a 12

Fase 9: el *cliente* solicita a la entidad de certificación de su banco (en adelante, *banco emisor*) su clave pública para enviarle un mensaje solicitándole el envío del *software* requerido para la posterior emisión de dinero electrónico.

Fase 10: la entidad de certificación envía al *cliente* la clave pública del *banco emisor*.

Fase 11: el *cliente* realiza el proceso de elaboración del mensaje autenticado que contiene la solicitud al *banco emisor* del *software* y la envía al banco.

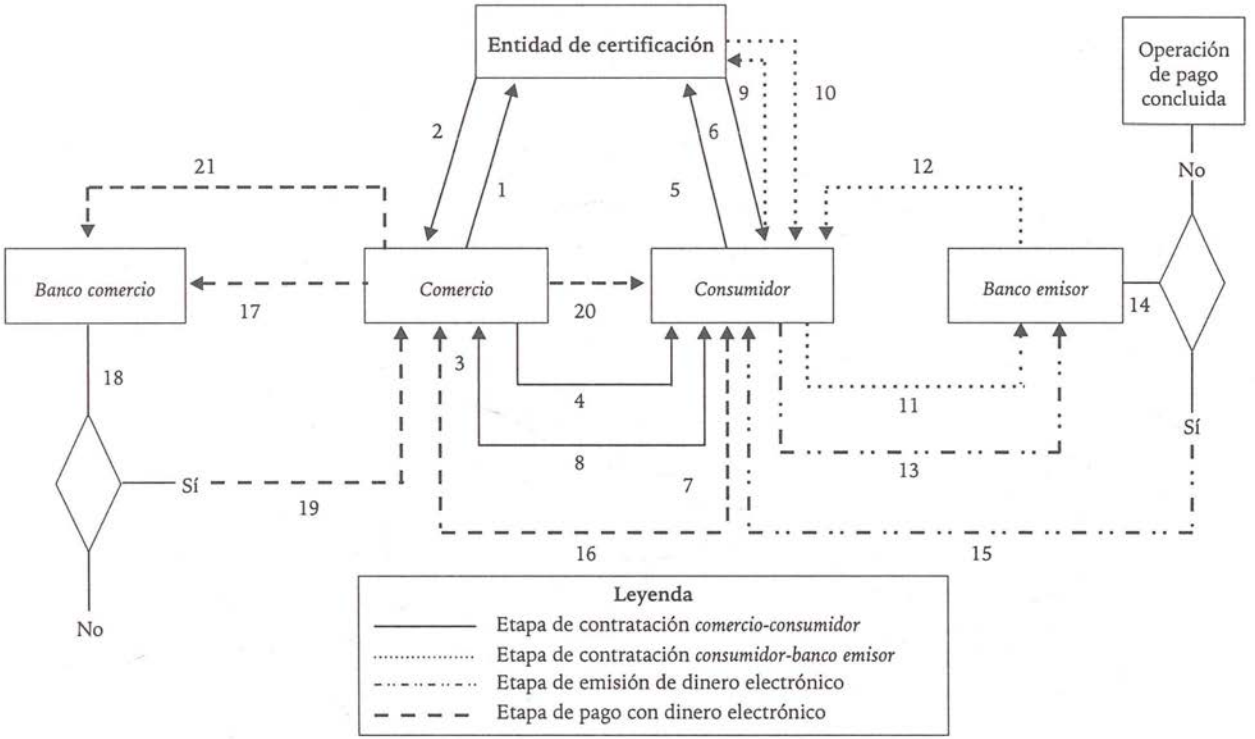
Fase 12: el *banco emisor* recibe el mensaje y acepta la solicitud del *cliente*, enviando el *software* correspondiente. Con ese fin, elaborará el mensaje autenticado correspondiente.

---

[10] Véase el cuadro A, p. 239.

[11] Véase el cuadro B, p. 239.

Etapas del modelo de transacción de comercio electrónico con el sistema de mensaje autenticado



5.3.3. Etapa de emisión de dinero electrónico. Fases 13 a 15

Fase 13: el *cliente* realiza el proceso de emisión del dinero electrónico empleando el *software* proporcionado por el *banco emisor* y envía el dinero generado a esta entidad. Para lograrlo elaborará el mensaje autenticado correspondiente.

Fase 14: el *banco emisor* verifica la identidad del cliente y su disponibilidad de fondos.

Fase 15: esta fase depende del resultado positivo de la verificación de la identidad del *cliente* y su disponibilidad de fondos. Si es así, se le otorga un valor al dinero electrónico generado, que es llamado dinero electrónico valorado y que es enviado al *cliente*. Para el envío del dinero electrónico valorado, el *banco emisor* generará el mensaje autenticado correspondiente.

5.3.4. Etapa de pago con dinero electrónico. Fases 16 a 21

Fase 16: una vez recibido el dinero electrónico valorado, el *cliente* envía el importe correspondiente al *comercio* para cancelar el precio de los bienes adquiridos. Con este fin, elaborará el mensaje autenticado correspondiente.

Fase 17: después de recibir el dinero electrónico valorado, el *comercio* lo envía a su vez a su banco (en adelante, *banco comercio*), elaborando el mensaje autenticado correspondiente.

Fase 18: el *banco comercio* verificará la autenticidad del dinero electrónico valorado enviado —si no ha sido empleado antes— y la disponibilidad de fondos del *cliente*, para lo cual se deberá comunicar con el *banco emisor*.

Fase 19: si las verificaciones realizadas en la fase anterior han tenido un resultado positivo, el *banco comercio* comunicará este resultado al *comercio*.

Fase 20: conocido el empleo viable del dinero electrónico valorado que ha sido enviado, el *comercio* envía al *cliente* los bienes adquiridos.

Fase 21: una vez enviados los bienes por el *comercio*, solicita al *banco comercio* el depósito en sus cuentas del valor monetario

representado por el dinero electrónico con el que se le canceló el precio de los bienes.

Debemos realizar las siguientes precisiones respecto de este modelo:

- Puede ser aplicado a cualquier tipo de transacción de comercio electrónico en cualquiera de sus diferentes etapas.
- El orden en el cual se han realizado las 21 fases puede variar en todas las operaciones de comercio electrónico.
- En este modelo la entidad de certificación es la misma para todos los sujetos que intervienen. Sin embargo, puede darse el caso de que sean diferentes entidades de certificación.
- La división del proceso en cuatro etapas no necesariamente se repite en todas las transacciones comerciales que utilicen medios electrónicos. Esta división tiene un objetivo didáctico.

6. PRINCIPIOS QUE REGULAN EL FUNCIONAMIENTO DEL SISTEMA DE SEGURIDAD JURÍDICA EN EL COMERCIO ELECTRÓNICO

Los principios que a continuación desarrollaremos son los que le dan al SSJ las directrices de funcionamiento. No pretendemos afirmar que son los únicos sino los que más protagonismo podrían tener. Pueden ser complementados por otros principios.

6.1. Principio de neutralidad tecnológica

De acuerdo con este principio, los diversos avances tecnológicos que con el transcurso del tiempo reemplacen a los medios tecnológicos que actualmente tengan la condición de medio de seguridad tendrán la condición de tales en tanto cumplan con los mismos objetivos del medio tecnológico reemplazado y con los mismos estándares de calidad.

Según Barzallo, «[...] la teoría de la neutralidad tecnológica propugnada por la UNCITRAL [...] [opta por] la no definición de estándares tecnológicos en las legislaciones internas, ya que en el

avance de la tecnología, la ley puede quedar obsoleta en cuestión de meses».[12]

Como vemos, este principio no solo se aplica al SSJ sino, también, al aspecto normativo de los diversos países. Esto se debe a dos motivos. En primer lugar, impedir la obstaculización del comercio electrónico por la dificultad del Derecho de adaptarse a los cambios tecnológicos. En segundo, procurar una uniformidad tanto tecnológica como legal en materia de *e-commerce* en la comunidad internacional.

Este principio tiene como objetivo evitar que, por el rápido avance tecnológico, los medios de seguridad jurídica que componen el SSJ no queden fuera de él. De esta manera, se dota de flexibilidad al sistema, al permitirle una fácil adaptación a las variaciones de la tecnología.

6.2. Principio de equivalencia funcional

Mediante este principio se pretende equiparar a los nuevos medios tecnológicos para entablar relaciones comerciales con los medios tradicionales.

Afirma Martínez Nadal que según este principio «[...] la firma digital consigue iguales, sino superiores efectos, que los de la firma manuscrita pues puede proporcionar integridad, autenticidad y, en definitiva, no rechazo de origen».[13]

Según González Ogaz, el principio de equivalencia funcional estipula que

> Los actos o contratos suscritos por medio de firma electrónica tienen la misma validez y producen iguales efectos que los celebrados por escrito y en soporte papel. Para darle mayor fuerza a esta idea, se establecen las

---

[12] BARZALLO, José Luis. «Los terceros de confianza en el comercio electrónico». En <http://vlex.com/redi/No._33_-_Abril_del_2001/8>.

[13] MARTÍNEZ NADAL, Apolonia. Comercio electrónico, firma digital y autoridades de certificación. Madrid: Civitas, 1998, p. 307.

> siguientes presunciones de derecho: a) se reputarán como escritos aquellos actos y contratos cuando la ley exija que los mismos consten por escrito; y, b) la firma electrónica se mirará como firma manuscrita para todos los efectos legales.[14]

Esta definición aporta dos premisas que nos parecen muy importantes para el funcionamiento del SSJ y que facilitan su flexibilidad.

La premisa de reputar como escritos los documentos electrónicos es útil porque no se puede pretender que el Derecho, en su esquema tradicional, elimine completamente sus formalidades y requerimientos. Si existiera una norma que obligara la formalidad por escrito de determinado acto o contrato, cuando fuera realizado en medios electrónicos, se consideraría como escrito automáticamente. De esta manera se crea un mecanismo que hace viable la convivencia de ambos sistemas.

Del mismo modo, la premisa de considerar la firma digital como una firma manuscrita para todos los efectos legales permite masificar el empleo de la primera, pues se le confiere los mismos efectos que a la firma manuscrita.

Pese a lo que sostienen los autores mencionados, consideramos que el principio de equivalencia funcional debe ser aplicado no solamente a la firma digital sino, también, a todos los medios de seguridad jurídica del SSJ. Estos medios reemplazan a un medio de seguridad tradicional; las entidades de certificación, a los notarios públicos; y los medios de pago electrónicos, al dinero. Por este motivo, bajo el alcance del principio de equivalencia funcional deberían estar incluidos todos los medios de seguridad de nuestro sistema de seguridad jurídica.

---

[14] González Ogaz, Cristóbal. «Algunos aspectos sobre el proyecto chileno de ley sobre firma electrónica y los servicios de certificación de firma electrónica». En <http://vlex.com/redi/No._35-_Junio_del_2001/9>.

6.3. Principio del valor probatorio del documento electrónico

Complementa al principio de equivalencia funcional, pues sería inútil que la firma digital fuera equivalente a una firma manuscrita si no tuviera valor probatorio. Según este principio, los documentos electrónicos empleados por los sujetos del comercio electrónico tendrán valor probatorio en tanto se hayan generado cumpliendo con los requisitos necesarios para su emisión. Este principio se complementa con los siguientes postulados de González Ogaz:[15]

6.3.1. Principio de prueba libre previa autorización judicial

Los documentos electrónicos se podrán presentar en juicio con las reglas generales de producción de la prueba. En todo caso, el juez deberá aceptar su presentación considerando los antecedentes de fiabilidad de la forma en que se generó, archivó o comunicó el documento y de la conservación de su integridad.

Esta regla supone el conocimiento por parte de los jueces de las comunicaciones electrónicas, condición aún muy lejana a nuestra realidad.

6.3.2. Principio de prueba tasada

Al documento electrónico se le reconoce el mismo valor probatorio que a los instrumentos privados o públicos, según su naturaleza, siempre que lleven una firma electrónica certificada por un prestador de servicios de certificación. En caso de no cumplirse con estos requisitos, el documento electrónico solo podrá considerarse base de una presunción judicial.

6.3.3. Principio de libre convicción

En los procedimientos en que el juez deba valorar la prueba según su propia convicción o según las reglas de la sana crítica —por ejemplo, en juicios de policía local— no se aplicarán los requisitos

---

[15] Ibíd.

mencionados en el punto referente al principio de prueba tasada de este trabajo. Con esta norma creemos que el legislador amplía demasiado la fuerza probatoria del documento electrónico, dejando la determinación de su valor en los jueces y en su cultura electrónica.

6.3.4. Autonomía de la voluntad

Las partes pueden pactar libremente los métodos de autenticación que usarán. En todo caso, los documentos generados por medio de estos procedimientos tendrán el valor de instrumento privado.

Ya que las leyes que regulan la prueba son de orden público, el legislador establece un límite importante para estos pactos privados. Estos acuerdos se considerarán no escritos si no cumplen con las condiciones de seguridad establecidas para la firma electrónica avanzada. Como se puede ver, esta libertad no es tan plena, puesto que se parte del mínimo de seguridad establecido por la ley.

6.4. Principio de actuación subsidiaria del Estado

Como hemos señalado repetidamente, el Estado no es lo suficientemente flexible como para adaptarse a la evolución tecnológica. Por esta razón, ante la rapidez de la evolución del *e-commerce* se hace necesario que el sector privado asuma determinadas funciones que son esenciales para garantizar la seguridad jurídica en las operaciones comerciales realizadas en Internet.

De este modo, según el principio de actuación subsidiaria del Estado, la actuación del Estado en la ejecución de determinadas funciones será dejada a cargo del sector privado, en tanto se garantice su adecuado cumplimiento.

Es necesario hacer ciertas precisiones respecto de este principio. En primer lugar, las funciones a las que se refiere son la función de certificación y la función de emisión del dinero.

En segundo lugar, se trata de un principio *numerus apertus*, pues es posible que se incorpore al SSJ otras funciones a cargo del Estado que este no pueda atender, debido al rápido desarrollo del comercio electrónico.

Asimismo, la actuación del Estado estará limitada a los casos en los que el sector privado no pueda intervenir de una manera confiable, es decir, será una actuación subsidiaria a la intervención privada.

Finalmente, el Estado tendrá siempre una participación indirecta, orientada a la fiscalización del ejercicio de las funciones delegadas en el sector privado.

7. CONCLUSIONES DEL CAPÍTULO

1. La concepción del Sistema de Seguridad Jurídico en el Comercio Electrónico (SSJ) responde a la participación limitada de los diversos medios de seguridad considerados individualmente. Por este motivo, tomando en consideración esta participación limitada, se considera que su funcionamiento óptimo es mejor en conjunto.

El SSJ es el conjunto de medios de seguridad electrónicos que interactúan en forma ordenada, de acuerdo a lo establecido por los principios de seguridad jurídica en el comercio electrónico, y cuyo objetivo es procurar la seguridad jurídica en las diversas operaciones de comercio electrónico que se pueden realizar mediante redes abiertas.

Debemos señalar que la concepción teórica del SSJ tiene como objetivo explicar, desde un punto de vista jurídico, el funcionamiento de los medios de seguridad en el comercio electrónico. Por lo tanto, en la práctica, no necesariamente la ejecución o funcionamiento de los medios de seguridad seguirá el mismo orden.

2. El SSJ está compuesto por los sujetos del comercio electrónico, los prestadores de servicios de certificación, las entidades financieras y los medios tecnológicos pertinentes. Será necesario que los sujetos que empleen el SSJ presten su consentimiento a someterse a sus principios y alcances para dotar de seguridad jurídica a las transacciones comerciales electrónicas que realicen.

3. La principal función del SSJ es dotar al comercio electrónico de seguridad jurídica para garantizar a los sujetos que lo practican la satisfacción de sus intereses y, del mismo modo, incentivar su masificación. Para lograrlo se vale del cumplimiento de las siguientes

funciones: identificación de los sujetos del comercio electrónico, identificación de los mensajes, vinculación de los sujetos, oponibilidad del pago electrónico y función probatoria. Existe otra función que los sujetos de comercio electrónico pueden incorporar, que es la función de intermediación.

4. El único objetivo del SSJ —dotar de seguridad jurídica a las operaciones de comercio electrónico— se logra en dos planos: en el primer plano garantiza que las operaciones de comercio llevadas a cabo por medios electrónicos surtan plenos efectos jurídicos y que sean oponibles y exigibles a las partes que las llevan a cabo. Para lograrlo se emplea el sistema de envío de mensajes autenticados, que consiste en el empleo conjunto de la firma digital y el certificado digital para el envío de mensajes. Con el empleo de este sistema está garantizada, en primer lugar, la identidad del autor mediante el certificado digital y, en segundo lugar, la integridad y confidencialidad de los mensajes, mediante el empleo de la firma digital. Así se logra la ejecución de la función de identificación de los sujetos y de los mensajes transmitidos. Este sistema de mensajes autenticados se aplica para cualquier operación de comercio electrónico, en cualquiera de sus etapas.

5. En el segundo plano, el SSJ garantiza la efectiva extinción de las obligaciones contraídas de dar suma de dinero, al hacer posible su oponibilidad al acreedor y a terceros. Esta garantía se logra con el empleo de los medios de pago electrónicos, que cumplen la función de oponibilidad.

6. Para el funcionamiento del SSJ será necesario que todas las partes que lo empleen cuenten con los medios tecnológicos adecuados. En otras palabras, deberán poseer una firma digital, un certificado digital y el *software* y *hardware* necesarios, así como los demás requerimientos tecnológicos que pudieran implementar.

7. El funcionamiento del SSJ está basado en los siguientes principios, que no son de aplicación exclusiva ni excluyente: el principio de neutralidad tecnológica, el principio de equivalencia funcional, el principio del valor probatorio del documento electrónico y el principio de actuación subsidiaria del Estado.

Del mismo modo debemos señalar que, de acuerdo con el avance tecnológico y el surgimiento de nuevas necesidades de seguridad jurídica, podrán ser incorporados otros principios.

8. La concepción del SSJ parte de un punto de vista sustantivo. En otras palabras, su aplicación está destinada a garantizar que el nacimiento de operaciones de comercio electrónico surtan plenos efectos para las partes que las lleven a cabo con éxito. Este sistema no ha sido diseñado contemplando las implicancias procesales que pudieran generarse si es necesaria una segunda fase que requiera el cumplimiento de las obligaciones contraídas por medio de mecanismos coercitivos.

No obstante, no pretendemos afirmar que el aspecto adjetivo no sea un elemento importante para que exista seguridad en las operaciones de comercio electrónico. Por el contrario, el aspecto adjetivo es indispensable, pues no es útil que se lleven a cabo las operaciones de comercio electrónico que surtan efectos jurídicos entre las partes si no existe la forma de exigir su cumplimiento mediante mecanismos coercitivos adecuados.

Como vemos, este trabajo tiene por objeto explicar el funcionamiento de los medios de seguridad tecnológicos desde un punto de vista jurídico sustantivo. Para esto hemos diseñado para el comercio electrónico un sistema de seguridad jurídica que abarca tan solo la fase de la generación o producción de actos de comercio, incluyendo su extinción mediante el pago electrónico. No abarca, entonces, una segunda y eventual fase de exigibilidad de estos actos de comercio en caso de incumplimiento. Será necesario, por tanto, el diseño de un mecanismo de solución de conflictos para el comercio electrónico en caso de que las obligaciones contraídas fueran incumplidas.

9. A fin de garantizar el funcionamiento eficiente del SSJ, los prestadores de servicios de certificación deberán adoptar fielmente los estándares en la calidad de sus servicios. En concordancia con el principio de actuación subsidiaria del Estado, este únicamente tendrá una participación indirecta en el cumplimiento de determinadas funciones, como la función de certificación o la emisión del dinero.

CAPÍTULO IV
Conclusiones

1. La creación de Internet —en sus inicios, un sistema de comunicaciones aplicado en actividades militares en los Estados Unidos de Norteamérica y actualmente un medio de comercio— ha planteado una serie de interrogantes en el ámbito jurídico, así como problemas y desafíos que deben ser encarados.

2. El comercio electrónico es, por excelencia, la aplicación económica de Internet. No existe transacción económica o comercial que en la actualidad no pueda ser realizada utilizando la red. En este hecho radica la importancia de su estudio y entendimiento, así como la solución a los problemas que se presenten con su desarrollo.

   Al ser un medio de comercio por excelencia, se utilizará en todo tipo de operaciones comerciales: locales, internacionales, al por mayor o menor o a domicilio, además de transacciones personales, familiares y empresariales, entre otras que no tengan necesariamente un carácter patrimonial. En definitiva, el potencial de Internet como medio de comercio es muy rico. La red de relaciones jurídicas que se puede tejer, por tanto, es muy extensa; en esto yace la importancia del Derecho como herramienta de regulación y control.

3. El problema central en torno al cual gira la problemática del comercio electrónico o *e-commerce* —en cuanto a su implementación y uso generalizado— es el de la seguridad en las operaciones de comercio que se realicen en Internet, que llamamos en este trabajo «la red».

   Este problema tiene su origen, en primer lugar, en la imposibilidad de identificar a las partes. En segundo lugar, en la posibilidad de que los mensajes transmitidos por medio de la red sean interceptados por terceros no autorizados, pues Internet se caracteriza por ser una red abierta, pública, a la cual puede tener acceso cualquier persona que cuente con la tecnología y el conocimiento necesarios. Esta posibilidad puede generar fraudes y delitos informáticos. Y, finalmente, en la posibilidad de que no se reconozca el pago realizado por medios electrónicos.

4. Así como el rol del Derecho en el comercio electrónico tendrá una función reguladora y controladora, tendrá que incentivar el empleo de este medio de comercio.

   Se ha señalado que el comercio electrónico presenta muchas desventajas, hecho que puede desmotivar su empleo, al menos en realidades sociales, económicas y culturales como la nuestra. Por este motivo, el Derecho deberá tener un rol que incentive el *e-commerce*, dotando a esta actividad de la seguridad jurídica necesaria. De esta manera, podrá dar confianza a los sujetos que opten por este medio de comercio, que ofrece más ventajas que desventajas.

5. El problema de la seguridad en el comercio electrónico tiene su origen principalmente en que se trata de una actividad comercial que hace innecesaria la proximidad física entre las partes que llevan a cabo un acto de comercio. Como hemos señalado, el *e-commerce* tiene una vocación de universalidad, es decir, personas de cualquier parte del mundo pueden entablar relaciones comerciales sin tener proximidad física y sin siquiera haberse conocido. Lo mismo ocurre con las operaciones comerciales locales: los sujetos no necesitan proximidad física, pues pueden

realizar cualquier operación comercial desde donde esté ubicada su computadora.

La ausencia de la proximidad física es el *quid* del problema de la seguridad jurídica en las operaciones de comercio electrónico. Si las partes están físicamente próximas y realizan una operación comercial, pueden comprobar la identidad de la otra parte, además de la idoneidad de los mecanismos que empleen para vincularse jurídicamente y para extinguir válidamente las obligaciones contraídas. Podrán, asimismo, exigir el pago del cumplimiento de estas obligaciones. Estas seguridades son imposibles en el comercio electrónico, ya que las partes, sin proximidad física, no pueden realizar estas comprobaciones.

Además de la falta de proximidad como origen del problema en el *e-commerce*, está la vulnerabilidad de los mensajes transmitidos por la red. Aun cuando existan medios para identificar a las personas que entablen relaciones comerciales por Internet, el medio por el que se envían los mensajes no es seguro: cualquier persona con los conocimientos y los medios tecnológicos necesarios puede tener acceso a ellos para conocer o modificar su contenido con fines ilícitos.

Por último, respecto del origen de la problemática del *e-commerce*, el hecho de que en ciertos casos no se reconozca por el Estado —y por ende legalmente— determinadas herramientas, como el dinero electrónico, la emisión de dinero electrónico o la función de certificación privada, entre otros, impide que el comercio electrónico siga su vocación de universalidad, pues se enfrenta con barreras interestatales y también dentro del Estado en que las partes se encuentren.

6. La tecnología ha ofrecido una respuesta a esta problemática implementado lo que hemos denominado «medios de seguridad jurídica para el comercio electrónico». Cada uno, o la combinación de algunos de ellos, cumple la función de solucionar los problemas que surgen. De este modo tenemos los siguientes problemas jurídicos y su medio de seguridad correspondiente:

Problema jurídico	Medio de seguridad
1. Identificación de las partes	**Certificado digital.** La identificación de las partes en el comercio electrónico por medio del certificado digital permite identificar a una persona determinada y asociarla con su firma digital.
2. Integridad de los mensajes	**Firma digital.** Este medio de seguridad, al emplear la criptografía asimétrica, permite que los mensajes o la información transmitidos por Internet no sean alterados durante su viaje por terceras personas.
3. Confidencialidad de los mensajes	**Firma digital.** Del mismo modo, el sistema de criptografía asimétrica empleado por este medio de seguridad evita no solamente que los mensajes sean alterados sino, también, que terceras personas accedan a ellos sin autorización del titular del mensaje.
4. Repudiación de los mensajes	**Firma digital - certificado digital.** Como hemos señalado, ambos medios permiten la integridad y confidencialidad de los mensajes, así como la identidad de las personas. Por lo tanto, al estar perfectamente asegurada la identidad de las personas y la de los mensajes enviados por la red, no será posible que el autor de un mensaje pretenda no reconocerlo, pues existen medios para determinar tanto su identidad como el contenido del mensaje que transmitió. Por lo tanto, la combinación de estos medios permite evitar el repudio de los mensajes transmitidos por Internet.
5. Pago de obligaciones	**Medios de pago electrónicos.** Nos referimos al pago de obligaciones de dar suma de dinero, de acuerdo con el estudio de los medios de pago electrónicos realizado para este trabajo. Los medios de pago electrónicos permiten el cumplimiento de estas obligaciones, al proporcionar un sistema de pagos confiable, eficiente y adecuados a la tecnología empleada.
6. Prueba del pago	**Medios de pago electrónicos.** La prueba del pago es otra de las preocupaciones al emplear medios electrónicos, en la medida en que el papel, el soporte tradicional, sigue muy arraigado en nuestras costumbres jurídicas y comerciales. Uno de los instrumentos con los que se puede probar el pago es la factura electrónica. Si bien este medio de seguridad permite la prueba electrónica de una transacción de pago determinada, será indispensable que cuente con determinadas regulaciones y con reconocimiento jurídico.

Debemos precisar que estos no son los únicos problemas jurídicos derivados de la práctica del comercio electrónico. Existen problemas adicionales como, por ejemplo, la libre competencia, los nombres de dominio, la publicidad desleal y conflictos de jurisdicción y de tribunales competentes, entre muchos otros. Sin embargo, los problemas mencionados han sido seleccionados intencionalmente dada la orientación que hemos dado a este trabajo.

Esta selección de los problemas jurídicos está relacionada con la formación adecuada de los actos jurídicos de comercio que se realicen en Internet para que puedan tener válidamente efectos jurídicos. Se ha pretendido describir, desde una perspectiva jurídica, los medios tecnológicos y su funcionamiento para que se realicen actos jurídicos válidos, eficaces y oponibles a las partes que los celebren.

Del mismo modo, este trabajo no apunta a una esfera contractual necesariamente, puesto que no es su objetivo determinar cuáles son los problemas y soluciones jurídicas de la contratación electrónica. Su fin, más bien, es establecer y explicar las implicancias jurídicas de los medios tecnológicos que hacen posible la celebración de actos de comercio—y, por ende, la contratación electrónica— de una manera segura.

7. En relación con la firma digital y el certificado digital, debemos realizar las siguientes precisiones.
   - La utilización de certificados emitidos por entidades de certificación —que vinculan de manera segura a una persona determinada con un par de claves— es necesaria para dar seguridad y fiabilidad al uso de firmas digitales en comunidades amplias y a gran escala, pues la vocación del comercio electrónico es universal. Con esto se soluciona los problemas de la integridad de los mensajes, de la autoría y, en definitiva, del rechazo de origen, es decir, la no-repudiación del mensaje.

- La regla de atribución de un mensaje electrónico a una persona determinada —verificando la asociación entre el titular de un certificado y su par de claves certificadas, regla que, en algunos casos, se convierte en presunción legal— solo tiene fundamento si las dos claves que están asociadas a la persona son únicas y no manipulables. En esta propiedad radica la importancia de la calidad de los sistemas de generación de claves, además la eventual responsabilidad de sus creadores, en caso de que sean defectuosos.
- Esta regla de atribución solo tendrá fundamento si, desde el punto de vista de organización y gestión del sistema de emisión de certificados digitales, se garantiza fehacientemente la comprobación de la identidad del autor del mensaje. Asimismo, si se consigue que la clave privada de firma esté en posesión (y, de ser el caso, en conocimiento) solo del autor del mensaje.

  Para lograrlo, desde el punto de vista jurídico, ha de considerarse, como función esencial del certificado, la vinculación certera de un par de claves a una persona determinada. Es imprescindible que esta vinculación sea fiable y segura. De ahí la importancia de los procedimientos de comprobación de la identidad del solicitante de un certificado. Por ello, la autoridad es responsable de adoptar ciertas medidas para determinar la identidad de la persona para quien emite un certificado.
- La existencia de distintos tipos de certificados y de firmas digitales con distintos niveles de seguridad, que son elementos comerciales, tiene también implicancias jurídicas. Supone efectos variados y la existencia de diferentes niveles de responsabilidad en función de la clase de firma y de certificado. No obstante, pese a esta acomodación de los efectos jurídicos a las prácticas comerciales, en ningún caso deben considerarse como certificados los productos comerciales que no cumplan con la función básica de distribución de las claves públicas (por ejemplo, en los certificados basados en un proceso

de solicitud y registro puramente *online*, en los que no hay comprobación alguna de identidad). De ahí la necesidad de establecer unos estándares mínimos para las autoridades de certificación y para los certificados.

En otro caso, si se permite y admite una excesiva flexibilidad en las prácticas comerciales, que facilite la actividad empresarial de las autoridades de certificación (necesarias para un comercio electrónico seguro), el sistema de certificados se desvirtuará. Si esto sucede, no se conseguirá su finalidad última, que —al margen de otros intereses comerciales parciales y subjetivos— es la seguridad del comercio electrónico, de interés absolutamente general y objetivo.

- Para que la regla de atribución tenga fundamento, también es esencial la obligación de custodia de la clave por parte de su titular. El incumplimiento de esta obligación es uno de los casos más frecuentes de revocación. Este procedimiento está destinado a declarar inoperativo un certificado de forma anticipada y plantea importantes problemas de determinación de responsabilidades.

  De esto se desprende que para el eficaz funcionamiento del SSJ será sumamente importante la participación y la colaboración de los sujetos del comercio electrónico. Estos tendrán obligaciones no necesariamente exigibles mediante normas legales sino vinculadas con una buena conducta comercial, por expresarlo de una manera.

  Por esta razón, sostenemos que los sujetos del comercio electrónico, como usuarios de los servicios de certificación, deberán ser sujetos de responsabilidad de acuerdo con determinados parámetros legales en los casos de empleo indebido de los servicios de certificación, como pueden ser una firma o un certificado digitales.
- La delicada cuestión de la responsabilidad derivada del sistema de certificados depende de una concreta opción político-legislativa, pero debe resolverse, en todo caso,

teniendo en cuenta los diversos intereses en juego y no solo los de la autoridad de certificación.

Debemos recalcar que esta opción político-legislativa respecto de la responsabilidad de las entidades prestadoras de servicios de certificación es de vital importancia. En efecto, equilibrará el SSJ que proponemos, al ser asumida la posición privatista frente al funcionamiento de las entidades prestadoras de servicios de certificación.

- Determinar la naturaleza de la responsabilidad de la autoridad de certificación puede consistir —sin llegar al extremo de la responsabilidad objetiva— en establecer una responsabilidad por culpa, pero con inversión de la carga de la prueba. De esta forma, para liberarse de responsabilidad, será la autoridad la que deba probar su diligencia.
- El riesgo potencialmente elevado, e incluso ilimitado, que asumen las autoridades de certificación justifica la existencia de limitaciones de distinta naturaleza y contenido, siempre y cuando no resulten abusivas (dejando, por ejemplo, vacío de contenido el certificado) y se realicen consideraciones semejantes cuando el responsable sea el suscriptor. Un ejemplo es la responsabilidad por pérdida de la clave privada. En este caso es conveniente la existencia de limitaciones cuantitativas.
- Los sellos temporales digitales fiables que permitan determinar el momento en el que se han llevado a cabo diversos hechos y acciones (la emisión de un certificado, de una declaración de prácticas de certificación, de una lista de certificados revocados, de un mensaje electrónico) son el tema de fondo que se debe resolver para un funcionamiento correcto del sistema de certificados.

8. El cumplimiento en las obligaciones contraídas por medios electrónicos puede efectuarse mediante la ejecución de diversos tipos de prestaciones, según el tipo operaciones comerciales

que se realicen. Podrán ejecutarse, entonces, prestaciones de hacer, de no hacer, de dar.

Sin embargo, este trabajo se ha centrado en las operaciones de comercio electrónico directo, en las que se ejecutan prestaciones de dar suma de dinero para realizar el pago de las obligaciones contraídas. La razón radica en que el objeto de nuestro estudio es el análisis de los medios electrónicos de seguridad jurídica en el comercio electrónico y, por consiguiente, el análisis de los medios de pago electrónico.

El pago en las obligaciones de hacer no es efectuado con medios de pago electrónicos, pues el deudor está obligado a la ejecución de un acto determinado. Respecto de las obligaciones de dar, no en todas las obligaciones de este tipo se emplearán los medios de pago electrónico, aun cuando el bien que es objeto de la prestación esté contenido en un soporte electrónico. En efecto, el cumplimiento de esta prestación se garantizará utilizando los medios de seguridad que garantizan la identidad de los mensajes y de su autor. Esta función corresponde a la firma digital y al certificado digital; no requiere de un medio de seguridad específico.[1]

Sin embargo, en las obligaciones de dar suma de dinero que se paguen con la entrega de dinero sí existe una particularidad específica. Para dotar de una mayor seguridad y rapidez a las operaciones de *e-commerce* se requiere de un tipo de moneda reconocida en todas partes del mundo y que, a su vez, permita la eficacia del pago y su oponibilidad. Se trata del dinero electrónico. Aquí no solo entran en juego los intereses de las partes que realizan una operación de comercio electrónico sino,

[1] Este es el caso del pago realizado mediante la entrega de un bien que puede estar contenido en un soporte material (un libro electrónico, por ejemplo). Por medio del sistema de mensajes autenticados se podrá garantizar la ejecución del pago mediante la entrega del libro electrónico empleando la red.

también, los intereses de las entidades financieras que emiten el dinero electrónico.

Por las razones señaladas existe un medio de seguridad específico para garantizar la viabilidad del pago electrónico. Este hecho nos ha motivado a restringir el presente estudio —en lo referente al pago de las obligaciones— a las obligaciones de dar suma de dinero.

9. Como podemos ver, existe una serie de problemas jurídicos que tienen su contrapartida en un medio o en una combinación de medios de seguridad. Sin embargo, estos medios o esta combinación de medios, tomados aisladamente, no cumplen la función de dotar de seguridad jurídica al comercio electrónico. Por este motivo, consideramos —como opción teórica— que estos medios forman parte de un sistema de seguridad jurídica en el comercio electrónico. Este sistema sí cumpliría con la función de garantizar la seguridad jurídica en las transacciones de *e-commerce*, en tanto se reúnan los requisitos para su funcionamiento y le sean aplicados sus principios reguladores.

10. La seguridad jurídica mencionada en el punto anterior tiene como fin lograr la certeza en lo que respecta a la consecución de los fines que los sujetos persigan al realizar operaciones de *e-commerce*.

El sentido que damos a certeza, en este contexto, es la posibilidad de determinar y garantizar razonablemente la identidad de los sujetos del comercio electrónico, además de la integridad y la confidencialidad de los mensajes transmitidos por la red, la eficacia del pago realizado por medios electrónicos y, complementariamente, la obtención de un medio de prueba.

Debemos precisar que la seguridad en nuestro SSJ tiene primordialmente una connotación de derecho sustantivo, abocada principalmente a lograr la certeza de la existencia de actos jurídicos válidos y oponibles frente a terceras personas. No está diseñado para ser aplicado en un plano de derecho adjetivo o procesal, plano que, si bien es indispensable para

conseguir el mismo objetivo de seguridad, deberá ser objeto de otra investigación.

Afirmamos entonces que la seguridad jurídica en el comercio electrónico puede pertenecer a dos categorías: la seguridad jurídica en un plano sustantivo y la seguridad jurídica en un plano adjetivo. El objeto de este estudio está centrado en la primera categoría.

11. El SSJ del comercio electrónico funciona por medio de una consecución de operaciones electrónicas simples que, seguidas unas de otras, otorgan seguridad jurídica a las operaciones de comercio electrónico.

    Sin embargo, debemos precisar que en la práctica estas operaciones no se realizan necesariamente consecutivamente sino en forma simultánea. La división de las operaciones de comercio electrónico y de los sistemas de seguridad jurídica en fases o etapas tiene como finalidad darles una explicación y una forma jurídica. Por esta razón, estas fases o etapas no son necesariamente las únicas. Pueden existir tantos tipos de etapas como criterios o formas para explicar jurídicamente el funcionamiento de los sistemas de seguridad jurídica en el *e-commerce*.

12. El SSJ que proponemos se vale de ciertos principios que regulan su funcionamiento. Estos principios —analizados y explicados en este trabajo— son los siguientes: el principio de neutralidad tecnológica, el principio de equivalencia funcional, el principio del valor probatorio del documento electrónico y el principio de actuación subsidiaria del Estado.

    Respecto de estos principios debemos señalar que no necesariamente son los únicos aplicables a nuestro sistema de seguridad. Dependiendo del desarrollo del comercio electrónico y de la aparición de problemas y necesidades distintas y, por lo tanto, de la aparición de nuevas funciones a cargo de nuestro sistema, se podrían incorporar nuevos principios. Debemos indicar también que estos principios no son necesariamente

exclusivos de nuestro sistema de seguridad. Algunos de ellos han sido extraídos de otros campos del Derecho y podrán ser aplicados a otros.

13. De los principios para el funcionamiento del sistema de seguridad que proponemos, el que tiene una trascendencia importante desde la percepción de la adaptación de estructuras jurídicas y comerciales es el principio de actuación subsidiaria del Estado.

De acuerdo con este principio, determinadas funciones a cargo del Estado, como la función de certificación y la emisión del dinero, no estarán a cargo del Estado en forma directa; su participación será indirecta. El fundamento de este principio es dotar de agilidad al comercio electrónico frente a la poca flexibilidad que el Estado ofrece frente a esta nueva forma de comercio. La función de certificación, a cargo principalmente de los notarios públicos en la actualidad, es una función que, si bien no es estrictamente pública, depende en gran medida del Estado. Esta dependencia no se da con las entidades de certificación que reemplazan a los notarios en el *e-commerce*. Lo mismo sucede con la emisión del dinero, función que actualmente está a cargo del Estado por medio del Banco Central de Reserva. Esto último no ocurriría en una operación de comercio electrónico, en la que las obligaciones son canceladas utilizando medios de pago electrónicos, como el dinero electrónico.

La participación de los notarios públicos en la función de certificación, o del Banco Central de Reserva en la emisión del dinero, no será viable en el comercio electrónico, teniendo en cuenta su vocación de universalidad. En efecto, su empleo retrasaría demasiado las operaciones de comercio celebradas. Pero no se trata únicamente de un tema de agilidad sino, también, de reconocimiento de entidades públicas a nivel interestatal.

Por esta razón, se hace necesario el cumplimiento de las funciones mencionadas, entre otras que pudieran aparecer, por parte de entidades que no estén vinculadas con el Estado,

para facilitar el reconocimiento de estas funciones en Estados distintos.

Se requiere, entonces, de un criterio o base para el reconocimiento internacional distinto del estatal. Este trabajo propone el reconocimiento ofrecido por el prestigio en el mercado de las entidades que presten servicios de certificación (emisión de firmas digitales, certificados digitales) y de las entidades que presten los servicios financieros en las operaciones de comercio electrónico (emisión de dinero digital, pago con dinero digital).

Actualmente, el prestigio de una compañía determinada es su mejor carta de presentación y su activo más valioso. Con él logra su reconocimiento internacional. En un mercado tan competitivo como el actual, en el que una compañía puede tener acceso a mercados internacionales fácilmente, el prestigio que obtenga y mantenga en estos mercados son el único medio que le permitirá tener vigencia y competitividad. Una muestra son los portales de venta de productos en línea como <http://www.amazon.com>, <http://www.jungla.com> o los proveedores de servicios de tarjetas electrónicas, como el Banco de Crédito y su tarjeta VíaBCP.

A pesar de lo anterior, no pretendemos afirmar que el único criterio de reconocimiento deba ser el prestigio de una empresa. También participa el Estado, pero de una manera subsidiaria e indirecta.

En el caso de la función de certificación, la función indirecta del Estado será el establecimiento de los requisitos y estándares que las entidades de certificación deberán reunir para su funcionamiento y que deberán estar adecuados a los estándares internacionales. No estará a su cargo la autorización previa para el funcionamiento de las entidades de certificación. En el caso de la función de emisión de dinero electrónico, la participación indirecta del Estado se basará en la supervisión de las entidades financieras a cargo de la emisión del dinero electrónico.

Por último, se requiere que el Estado no participe en la regulación ni en la consiguiente prescripción de los estándares mínimos con los que se prestarán los servicios de certificación. Opinamos que deberán ser entidades privadas —como, por ejemplo, la American Bar Association, la UNCITRAL o la Cámara de Comercio Internacional— las que cumplan con esta función de prescribir los estándares referentes a los servicios prestados que permitan la realización del comercio electrónico. De lo contrario, si el Estado estuviera a cargo de esta actividad, nos enfrentaríamos al problema del distinto reconocimiento de los estándares de un Estado a otro.

Como vemos, la participación indirecta del Estado es justificada y compensada.

14. Se desprende del punto anterior que la participación del Estado es necesaria en una etapa previa a la apertura del comercio electrónico. Esta participación se dará únicamente cuando el Estado dicte las normas que acojan los principios del SSJ en el comercio electrónico, recogiendo los principios mencionados, para flexibilizar la implementación de esta actividad comercial. Una vez dado este paso, la participación del Estado se conformará a lo descrito.

15. El SSJ propuesto implica necesariamente que los sujetos que lo empleen cumplan con ciertos requerimientos. Por un lado, prestar su consentimiento en el empleo del sistema y declarar su sometimiento expreso a sus principios y fundamentos. Por otra parte, contar con la tecnología adecuada (una firma digital, un certificado digital y el *software* y el *hardware* necesarios).

16. Analizando la implementación de nuestro SSJ en el comercio electrónico, en nuestra realidad, nos damos cuenta de que en la actualidad no es muy viable debido, principalmente, a los costos excesivos.

Un microempresario o un pequeño o mediano empresario peruano que quiera ofrecer sus productos o servicios no solo

dentro de nuestro territorio sino en cualquier parte del mundo, mediante su sitio web, deberá invertir en su certificado con protocolo de seguridad SET 590 dólares anuales. Este certificado no incluye la instalación en el servidor web, cuyo servicio cuesta aproximadamente 300 dólares.[2] A pesar de esto, el proveedor que comercializa estos certificados acepta como único *software* para crear los catálogos y tener acceso al portal de pagos un sistema desarrollado por IBM, denominado Wesphere Payment Manager, que tiene un costo de 16.547 dólares. Este monto incluyen el IGV pero no contempla el desarrollo ni el mantenimiento del catálogo de productos y servicios de la tienda virtual.

Concluimos entonces que los precios de los productos de certificación, indispensables para el funcionamiento del comercio electrónico, no le permiten mayor expansión, puesto que para cualquier microempresario o pequeño o mediano empresario esta inversión es difícil de financiar, por no decir imposible.

Existe, sin embargo, otra vía para que los comerciantes implementen sus portales de venta en Internet. Si una empresa no tiene la capacidad para adquirir el sistema de IBM puede recurrir a algún intermediario. Por ejemplo, una subsidiaria de la compañía española proveedora de servicios telefónicos en nuestro país, que cobra una cuota de inscripción de 823 dólares y un pago mensual de 140 dólares (más el IGV) por el uso de su portal de pagos y, por si fuera poco, una comisión del 2% por cada transacción aprobada, adicional al 5% del descuento de la operadora de la tarjeta de crédito.[3] Esta segunda alternativa tampoco es prometedora como un incentivo a la actividad comercial por medios electrónicos como Internet.

---

[2] MACHADO, Jorge. «¿Es fácil hacer comercio electrónico en el Perú?» En <http:// www.portalti.com/articulos/nov-01/comelectro_peru_20nov01.html>.

[3] Ibíd.

dentro de nuestro territorio sino en cualquier parte del mundo, mediante su sitio web, deberá invertir en su certificado con protocolo de seguridad SET 590 dólares anuales. Este certificado no incluye la instalación en el servidor web, cuyo servicio cuesta aproximadamente 300 dólares.[2] A pesar de esto, el proveedor que comercializa estos certificados acepta como único *software* para crear los catálogos y tener acceso al portal de pagos un sistema desarrollado por IBM, denominado Wesphere Payment Manager, que tiene un costo de 16.547 dólares. Este monto incluyen el IGV pero no contempla el desarrollo ni el mantenimiento del catálogo de productos y servicios de la tienda virtual.

Concluimos entonces que los precios de los productos de certificación, indispensables para el funcionamiento del comercio electrónico, no le permiten mayor expansión, puesto que para cualquier microempresario o pequeño o mediano empresario esta inversión es difícil de financiar, por no decir imposible.

Existe, sin embargo, otra vía para que los comerciantes implementen sus portales de venta en Internet. Si una empresa no tiene la capacidad para adquirir el sistema de IBM puede recurrir a algún intermediario. Por ejemplo, una subsidiaria de la compañía española proveedora de servicios telefónicos en nuestro país, que cobra una cuota de inscripción de 823 dólares y un pago mensual de 140 dólares (más el IGV) por el uso de su portal de pagos y, por si fuera poco, una comisión del 2% por cada transacción aprobada, adicional al 5% del descuento de la operadora de la tarjeta de crédito.[3] Esta segunda alternativa tampoco es prometedora como un incentivo a la actividad comercial por medios electrónicos como Internet.

---

[2] MACHADO, Jorge. «¿Es fácil hacer comercio electrónico en el Perú?» En <http:// www.portalti.com/articulos/nov-01/comelectro_peru_20nov01.html>.

[3] Ibíd.

A diferencia de lo que ocurre en nuestro país, en otros países como Estados Unidos y Canadá se brindan los servicios de portales de pago para transacciones de comercio electrónico en servidores seguros con el protocolo SSL y sistemas propietarios antifraudes a precios sumamente competitivos. Sus tarifas varían, con pagos de inscripción desde 495 a 595 dólares, por única vez, y de 3,85% a 3,95% de descuento al monto de la venta, más un cobro de 0,50 a 1,50 dólares por cada transacción y un pago mensual de 25 a 35 dólares por el uso de su portal de pagos.[4]

En estos sistemas no es necesario adquirir ningún certificado SET o SSL, que son desarrollados y emitidos por la misma corporación. Mediante estos portales de pago se pueden aceptar transacciones con tarjetas Visa, MasterCard, American Express y Discovery. Por si fuera poco, estos portales de pago no requieren que la empresa peruana abra una cuenta corriente bancaria ni que tenga presencia legal en el extranjero. Cada 15 días el monto de las ventas es remitido a la cuenta corriente de su banco local peruano, menos el costo de la transferencia bancaria (*wire transfer*).

17. Del punto anterior se desprende que, para la expansión del comercio electrónico en nuestro país, será necesaria la intervención y la participación tanto del sector privado —en la implementación de sistemas novedosos y competitivos, y de fácil acceso en el mercado— como del Estado, al dictar normas que favorezcan e incentiven esta actividad.

18. El concepto de seguridad en el comercio electrónico es complejo. Está compuesto de una serie de factores políticos, sociales, económicos y jurídicos. La solución que el Derecho pueda dar a los problemas jurídicos de esta actividad económica no

[4] Ibíd.

será suficiente por sí sola. Deben confluir todos los factores involucrados.

19. Nuestro SSJ es un planteamiento teórico que busca, en primer lugar, someter la seguridad en el comercio electrónico a un molde jurídico para analizar la perspectiva jurídica de los medios de seguridad electrónicos, que la tecnología ha proporcionado.

    Se trata de un aporte teórico de dar una explicación jurídica de la seguridad en materia de comercio electrónico. El sistema de seguridad que proponemos no es un sistema perfecto; tiene aspectos tanto positivos como negativos. Este hecho se debe a que se basa en el empleo de medios de seguridad que tienen a su vez ventajas y desventajas. Su superioridad radica en que su concepción como un sistema integrado reduce las desventajas de cada medio considerado individualmente. Sin embargo, lo que nunca se podrá lograr —a nuestro parecer— es la elaboración de un sistema de seguridad perfecto en un 100%, ya que siempre existirá el riesgo de su vulneración.

    Con este trabajo pretendemos dar inicio e incentivar una serie de investigaciones posteriores sobre los medios de seguridad desde una perspectiva integral, como un sistema, complementando y mejorando nuestra propuesta.

Bibliografía

1. Sistemas de seguridad

1.1. Criptografía

CÁNOVAS REVERTE, Óscar

1999 «Las claves criptográficas». *Boletín del Criptonomicón*, n.° 55. En <http://www.iec.csic.es/criptonomicon/articulos/expertos55.html>.

HERRERA JOANCOMARTI, Jordi

1999 «Criptografía de clave pública». *Boletín del Criptonomicón*, n.° 44. En <http://www.iec.csic.es/criptonomicon/articulos/expertos44.html>.

MICROSOFT CORPORATION

2001 «Introducción a la infraestructura de claves públicas de Windows 2000». Última actualización: 9 de marzo. En <http://www.microsoft.latam/technet/ecommerce/default.asp>.

SÁEZ I MORENO, Germán

1999 «El azar en la criptografía». *Boletín del Criptonomicón*, n.° 52. En <http://www.iec.csic.es/criptonomicon/articulos/expertos52.html>.

SÁNCHEZ ALMEIDA, Carlos

2000 «La criptografía como derecho». En <http://publicaciones.derecho.org/redi/No._23_-_Junio_del_2000/4>.

1.2. Medios de pago

MALTESE, Mariano
s. a. «El pago electrónico en la Argentina». En <http://www.vlex.ar/cn/Derecho_Inform@tico/12>.

ORTEGA DÍAZ, Juan Francisco
2001 «El cumplimiento del pago por medios electrónicos». En <http://www.vlex.com/redi/No._36_-_Julio_del_2001/9>.

RICO CARRILLO, Mariliana
1999 «El pago mediante tarjetas en el comercio electrónico a través de Internet». Tesina presentada para la obtención de suficiencia investigadora, requisito previo a la obtención del título de doctor en Derecho. Madrid: Universidad Carlos III.

1.3. Biometría

s. a. «Biometría: verdades y ficciones». Trad. de Ángel Galindo. En <http://www.kriptopolis.com/criptograma/0004_5.html>.
s. a. «De la contraseña a la identificación biométrica: La seguridad en el comercio electrónico». En <http://www.tecnipublicaciones.com/teleinf/actualidad/seguridad.asp?opcion=informe>.

GONZÁLEZ RODRÍGUEZ, Joaquín
2000 «Identificación biométrica». *Boletín del Criptonomicón*, n.º 73. En <http://www.iec.csic.es/criptonomicon/articulos/expertos73.html>
s. a. «Más sobre biometría». Trad. de Ángel Galindo. En <http://www.kriptopolis.com/criptograma/0005_7.html>.

2. COMERCIO ELECTRÓNICO

CALDERÓN RODRÍGUEZ, Cristian L.
s. a. «El comercio electrónico: nueva *lex mercatoria* del comercio internacional». En <http://www.alfa-redi.org/revista/data/27-9.asp>.

COÁGUILA, Carlos Soto
2003 «El comercio electrónico en el derecho peruano». En *Instituciones de derecho privado*. Tomo III: *Comercio electrónico*. Ara Editores. Editorial Temis S.A.

COVA ARRIA, Luis
2000 «Obstáculos legales para la implementación de la ley modelo de UNCITRAL sobre comercio electrónico en los países de derecho civil». Ponencia presentada en el «Tercer Congreso Internacional de Derecho Civil Comercio Electrónico, Contratación y Daños». Arequipa, 17 y 18 de noviembre de 2000.

GONZÁLEZ GALLEGO, Francisco
s. a. «Comercio electrónico: aspectos técnicos: privacidad y firma electrónica». En <http://www.tel.uva.es/~fgongal/ce/trabajo/tecnic. htm>.
s. a. «Confianza y fidelización en el comercio electrónico». En <http://www.tel.uva.es/~fgongal/ce/trabajo/critica.htm>.

JOVANÉ, Lissy
s. a. «Problemas jurídicos del comercio electrónico». En <http://www.legalinfo-panama.com/articulos/articulos_13g.htm>.

LORENZETTI, Ricardo Luis
2003 «El comercio electrónico. La teoría general». En *Instituciones de derecho privado*. Tomo III: *Comercio electrónico*. Ara Editores. Editorial Temis S. A.

MAESTRE, Javier A. y Carlos SÁNCHEZ ALMEIDA
s. a. «Análisis de la directiva sobre comercio electrónico (servicios de la sociedad de la información.» En <http://comunidad.derecho.org/redi/lssi.txt>.
s. a. «¿Qué es comercio electrónico?» En <http://ute.edu.ec/~mjativa/ce/que-es-com-elec.html>.

RICO CARRILLO, Mariliana
1999 «El pago mediante tarjetas en el comercio electrónico a través de Internet». Tesina presentada para la obtención de suficiencia investigadora, requisito previo a la obtención del título de doctor en Derecho. Madrid: Universidad Carlos III.

3. FIRMAS Y CERTIFICADOS DIGITALES

3.1. Entidades de certificación

BARZALLO, José Luis
2001 «Los terceros de confianza en el comercio electrónico». En <http://vlex.com/redi/No._33_-_Abril_del_2001/8>.

ITAMAR ARRUDA, Júnior
2001 «Documentos eletrônicos, autoridades certificadoras e legislação aplicable». En <http://vlex.com/redi/No._35_-_Junio_del_2001/5>.

JIJENA LEIVA, Renato
2001 «Firma digital y entidades certificadoras. Regulación legal en la administración pública chilena». En <http://publicaciones.derecho.org/redi/No._35_-_Junio_del_2001/2>.

MARTÍN REYES, María de los Ángeles
2001 «Las entidades de certificación». En <http://vlex.com/redi/No._35_-_Junio_del_2001/11>.

MARTÍNEZ NADAL, Apolonia
1998 *Comercio electrónico, firma digital y autoridades de certificación*. Madrid: Civitas.
2000 *La ley de firma electrónica*. Madrid: Civitas.

MUÑOZ ESQUIVEL, Oliver
2001 «Actividad de las entidades de certificación frente a la función notarial». En <http://vlex.com/redi/No._35_-_Junio_del_2001/15>.

3.2. Firma digital

CABALLERO GIL, Pino
1998 «Cómo funcionan las firmas digitales». En <http://www. iec.csic.es/criptonomicon/articulos/expertos32.html>.

CUERVO, José
1998 «La firma digital y entidades de certificación». En <http://www.informatica-juridica.com/trabajos.asp>.

ESCOBAR ROZAS, Freddy
s. a. «La firma electrónica en la ley peruana». En <http://v2.vlex.com/es/ppv/doctrina/resultados.asp?query_doc=107888&n_orden=0&>.

FERNÁNDEZ PEPPER, Marta
2000 «La ley de firmas y certificados digitales». En Gestión, 6 de noviembre.

GONZÁLEZ OGAZ, Cristóbal
2001 «Algunos aspectos sobre el proyecto chileno de ley sobre firma electrónica y los servicios de certificación de firma electrónica». En <http://vlex.com/redi/No._35_-_Junio_del_2001/9>.

RAMOS SUÁREZ, Fernando
s. a. «La firma digital: aspectos técnicos y legales». En <http://www.marketingycomercio.com/numero14/00abr_firmadigital.htm>.
2001 «Cómo aplicar la nueva normativa sobre firma electrónica». En <http://publicaciones.derecho.org/redi/No._19_-_Febrero_del_2001/1>.

3.3. Certificados digitales

MARTÍNEZ, Fernando
1999 «Qué son los certificados digitales». En <http://www.iec.csic.es/criptonomicon/articulos/expertos51.html>.

3.4. Varios

ARGUEDAS, Ysella
s..a. «La seguridad en Internet es posible».

RODRÍGUEZ, Katitza
s. a. «Entrevista a Fernando Ocampo. Comentarios al proyecto de reglamento de la ley de firmas y certificados digitales». En <http://www.v-lex.com>.

4. INTERNET

BARRIOS OSORIO, Omar Ricardo
2001 «Internet y Derecho. Fundamentos de una relación». En <http://vlex.com/redi/No._35_-_Junio_del_2001/12>.

BLASCO, Jordi
s. a. «Problemas jurídicos derivados del uso de Internet». En <http://www.derecho.com/boletin/articulos/articulo0035.htm>.

GONZÁLEZ GALLEGO, Francisco
s. a. «Comercio electrónico. ¿Para qué sirve Internet?». En <http://www.tel.uva.es/~fgongal/ce/trabajo/critica.htm>.
2001 *Informática y Derecho. Aportes de doctrina internacional*. Volumen VIII. Internet. Buenos Aires: LexisNexis Desalma.

IRIARTE AHÓN, Erick
s. a. «Algunas reflexiones sobre el desarrollo del Internet». En <http://www.alfa-redi.org/revista/data/26-7.asp>.

RAMOS SUÁREZ, Fernando
2000 «Implicaciones jurídicas de la Tecnología Wap». En <http://vlex.com/redi/No._22_-_Mayo_del_2000/7>.
2001 «Internet y comercio electrónico». En <http://www.itu.int/newsroom/wtd/2001/FeatureE-commerce-es.html>.
2001 «La singularidad en Internet». En <http://www.itu.int/newsroom/wtd/2001/ExecutiveSummary-es.html>.

5. SOCIEDAD DE LA INFORMACIÓN

CARO FIGUEROA, Luis Alberto
s.a. «La sociedad de la información». En <http://www.kumiko.com.ar/luiscaro/socinform.htm>.

MERAYO PÉREZ, Arturo
1997 «La nueva sociedad de la información: tendencias, riesgos y soluciones». En <http://bocc.ubi.pt/pag/merayo-arturo-sociedad-informacion.html>.

El sistema de seguridad jurídica
en el comercio electrónico
se terminó de imprimir en los talleres de
Gráfica Delvi S. R. L.
Av. Petit Thouars 2009 - Lince
en el mes de febrero de 2005

PRÓXIMAS PUBLICACIONES

Reglas simples para un mundo complejo
Richard A. Epstein
Coedición con la Asociación Civil
Ius et Veritas

Senderos que se bifurcan.
Dilemas y retos de la sociedad
de la información
Eduardo Villanueva Mansilla

Hidráulica general
Wendor Chereque

Fondo Editorial de la PUCP
Plaza Francia 1164, Lima 1 – Perú
Teléfonos: (51 1) 330-7410, 330-7411
Fax: (51 1) 330-7405
Correo electrónico: feditor@pucp.edu.pe
www.pucp.edu.pe/publicaciones/fondo_ed/

Los avances científicos y tecnológicos plantean nuevos desafíos a los legisladores y especialistas del Derecho, en gran medida porque el actual desarrollo de los medios de información y comunicación electrónicos ha creado y sigue creando espacios alternativos para buena parte de las relaciones sociales ya conocidas. De este modo, aunque estas puedan ser sustancialmente las mismas, sus canales y medios cambian, y las formas en que la ley las regula dejan de ser adecuadas. Este es el caso del comercio, cuya variante electrónica supone características y formas que hacen necesario construir un sistema jurídico nuevo o adaptar el vigente, con el fin de asegurar el pleno cumplimiento de los compromisos asumidos en las relaciones comerciales así establecidas. El reto que enfrenta la presente obra es articular un posible sistema de seguridad jurídica que, tomando en cuenta las características propias de los medios electrónicos, otorgue validez y seguridad legales a las transacciones realizadas a través de ellos.

ISBN 9972-42-677-7