Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

SCIENZE GIURIDICHE

Ciclo XXX

**Settore Concorsuale: 12/H3**

**Settore Scientifico Disciplinare: IUS/20**

# IMPATTO DELLA NUOVA REGOLAZIONE EUROPEA IN MATERIA DI IDENTIFICAZIONE ELETTRONICA E SERVIZI FIDUCIARI NELL'AMBITO DELLA CONTRATTAZIONE PRIVATA DOTATA DI FIRMA ELETTRONICA

-

# IMPACTO DE LA NUEVA REGULACIÓN EUROPEA SOBRE IDENTIFICACIÓN ELECTRÓNICA Y SERVICIOS DE CONFIANZA EN EL ÁMBITO DE LA CONTRATACIÓN PRIVADA DOTADA DE FIRMA ELECTRÓNICA

**Presentata da: Juan Francisco Rodríguez Ayuso**

**Coordinatore Dottorato** **Supervisore**

**Andrea Morrone** **Giovanni Sartor**

**Esame finale anno 2018**

*A mi familia,*

*gracias a vosotros todo fue posible.*

«Nada es suficiente para quien
lo suficiente es poco»

EPICURO DE SAMOS
(*Exhortaciones, 68*)

# ABSTRACT

Il presente lavoro ha come obiettivo quello di analizzare l'evoluzione e il quadro giuridico attuale di un'innovativa istituzione all'interno del nostro ordinamento giuridico, nazionale e comunitario. Parliamo della firma elettronica, essenziale servizio fiduciario che acquisisce una nuova rilevanza seguito dell'entrata in vigore del Regolamento (UE) nº 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, regolamento riguardante l'identificazione elettronica e i servizi fiduciari per gli scambi elettronici nel mercato interno e la conseguente normativa di attuazione. Dal 2014 questo nuovo Regolamento costituirà il quadro legale fondamentale dell'Unione Europea, come conseguenza dell'abrogazione messa in atto dalla Direttiva 1999/93/CE del Parlamento Europeo e del Consiglio, del 13 dicembre 1999, e con la quale si fissa un quadro comunitario per la firma elettronica.

Particolare attenzione sarà rivolta all'influsso che questo scenario legale emergente conferisce alla contrattazione elettronica tra privati. Infatti, quale essenziale servizio della società dell'informazione, e considerando altresì la sua progressiva rilevanza nel mercato comunitario e globale, la contrattazione elettronica si servirà dell'incorporazione o del costante rinnovamento di determinati strumenti, quali la firma elettronica, che contribuiscano a creare certezza e sicurezza in quelle transazioni che, ricorrendo ad essa, avvengono tramite la manifestazione della volontà e il consenso dei contraenti in relazione al contenuto stesso dell'accordo negoziale.

## ABSTRACT

The main aim of the present study is to analyze the evolution and the current legal framework of a new institution within our national and communitarian legal system. We are talking about the electronic signature, an essential trust service which acquires a renewed vision as the direct consequence of the entry into force of the 910/2014 (EU) Regulation of the European Parliamentary and of the Council 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and its development normative. This new Regulation constitutes the fundamental legal framework from 2014 onwards in the sphere of the European Union as a consequence of the abolition executed by the Directive 1999/93/CE of the European Parliamentary and of the Council of 13 December 1999 on a Community framework for electronic signatures.

More precisely, special attention will be given to the influence that this emerging legal context prints into the electronic contracting among individuals. Indeed, as essential information society service and its progressive relevance within the global and communitarian market, the electronic contracting needs a constant incorporation or renewal of elements such as the electronic signature that contributes to generate trust and security in the transactions that, under their own choice, take place throughout the participants' consent related to the negotiating contents' agreement.

# ÍNDICE

## CAPÍTULO SEGUNDO

## VALIDEZ Y EFICACIA DE LOS CONTRATOS PRIVADOS

## CAPÍTULO TERCERO

## FIRMA ELECTRÓNICA COMO MEDIO DE PRUEBA DE CONTRATOS ELECTRÓNICOS DE NATURALEZA PRIVADA

# CAPÍTULO CUARTO
# ELEMENTOS SUBJETIVOS DEL SISTEMA DE FIRMA ELECTRÓNICA

# NOTA PRELIMINAR

Una nota preliminar a un estudio universitario suele caracterizarse por ser la parte menos meditada y, al mismo tiempo, la más sentimental e íntima del mismo. Es aquella parte que el autor escribe al final, orgulloso por el resultado obtenido, que deja de ligarse exclusivamente a cuestiones académicas para identificarse como uno de los mejores ejemplos de esfuerzo empleado para conseguir un objetivo, de ahí la satisfacción que encierra. Es por ello que, quien se aproxime al contenido de la presente Tesis Doctoral, dejará de creer que esta sección se trata de un mero formulismo para percibir con claridad que lo que en ella se expresa es cierto y que la satisfacción y esfuerzo aludidos no son sino el fruto de una labor conjunta de quien suscribe estas líneas y de todas aquellas personas que, SIEMPRE E INCONDICIONALMENTE, han estado detrás, aquellas personas sin cuya ayuda esto nunca hubiera sido posible.

A lo anterior, si bien intrínsecamente relacionado, se une la dicha de haber sido becario del Real Colegio de España en Bolonia. Por ello, la primera de las personas a la que debo expresar mi más profunda gratitud es a nuestro cardenal, DON GIL ÁLVAREZ DE ALBORNOZ, cuyo generoso y eterno legado me han permitido, a nivel personal, vivir una de las mejores experiencias de mi vida y, en un plano puramente académico o profesional, poder decir con honra que soy *Bolonio* y que he formado parte de la madre de todas las universidades, la *Alma Mater Studiorum*. Gracias igualmente, como no, a nuestro rector, DON JUAN JOSÉ GUTIÉRREZ ALONSO, por hacer que la huella, tantas veces anunciada, del admirado DON JOSÉ GUILLERMO GARCÍA VALDECASAS sea, al menos, más liviana, acompañándonos en todo momento con su atención, ayuda y generosidad. Y gracias también a todos los compañeros que han pasado por el Colegio a lo largo de mis dos años de estancia, especialmente a aquellos con los que he podido convivir de manera permanente y estrecha y sin los cuales esto no habría podido ser lo que es.

Expresar mi agradecimiento a todos los compañeros de doctorado y a quien ha sido mi director en este trabajo, el profesor DON GIOVANNI SARTOR. Gracias sinceras por permitir que todas estas páginas puedan ver la luz.

Además, tengo que dejar constancia de la inestimable y desinteresada predisposición mostrada por los admirados profesores DON MANUEL FERNÁNDEZ SALMERÓN, antiguo colegial de nuestro Real Colegio de España y cuya enorme amabilidad agradezco, y DON JOSÉ LUIS PÉREZ-SERRABONA GONZÁLEZ, a quien tuve ocasión de conocer personalmente en Bolonia, pero cuyo nombre y buen hacer no dejé de escuchar sino desde mucho tiempo antes.

Más recientemente, no puedo mostrar sino mi más sincera gratitud hacia todas las personas con las que trabajo diariamente en Málaga. Gracias por darme esta oportunidad, por permitir que desde un principio forme parte de esto como si llevara toda la vida y por hacer posible que cada día me levante feliz y agradecido por lo que hago. También a mi primo FRANCISCO JOSÉ, porque el futuro se nos presenta duro, pero prometedor e ilusionante.

Gracias A TODA MI FAMILIA, especialmente a MIS PADRES y a MIS HERMANOS, por ser el principal soporte y eje en torno al cual se articula mi vida y sin los cuales ni esto ni nada de lo que soy, hago y haré hubiera sido posible. Nada me puede hacer más feliz que DIOS me haya regalado la posibilidad de que podáis ver el resultado de vuestros incansables esfuerzos.

Y a ti, PILAR, por ser un regalo caído del cielo, por tu paciencia, por tu cariño y por permitir que me dé cuenta de que las cosas más importantes son aquellas que no se ven sino que se sienten.

El autor.

Córdoba, a 1 de noviembre de 2017

# ABREVIATURAS

## A

| | |
|---|---|
| A2A | *Administration to Administration* |
| A2B | *Administration to Business* |
| A2C | *Administration to Consumer* |
| AALGT | Ley 11/1998, de 24 de abril, general de telecomunicaciones |
| ACCNMVAS | Acuerdo de 16 de noviembre de 2011, del Consejo de la Comisión Nacional del Mercado de Valores, en relación con la adaptación del Sistema CIFRADOC/CNMV a los servicios de certificación y firma electrónica reconocida y se crea el registro telemático de la CNMV |
| ACCNMVIS | Acuerdo del Consejo de la Comisión Nacional del Mercado de Valores de 11 de marzo de 1998 para la implantación del sistema CIFRADOC/CNMV |
| AEPD | Agencia Española de Protección de Datos |
| ALECiv | Real Decreto de 3 de febrero de 1881 por el que se aprueba el proyecto de reforma de la Ley de enjuiciamiento civil |
| ALGT | Ley 32/2003, de 3 de noviembre, general de telecomunicaciones |
| ALOPDCP | Anteproyecto de Ley Orgánica de protección de datos de carácter personal |

| | |
|---|---|
| ALSEC | Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza |
| AP | Audiencia Provincial |
| ARDRDM | Real Decreto 553/2004, de 17 de abril, por el que se reestructuran los departamentos ministeriales |
| ARPA | *Advanced Research Projects Agency* |
| ARPANET | *Advanced Research Projects Agency NETwork* |

**B**

| | |
|---|---|
| B2A | *Business to Administration* |
| B2B | *Business to Business* |
| B2C | *Business to Consumer* |
| BOE | Boletín Oficial del Estado |

**C**

| | |
|---|---|
| C2A | *Consumer to Administration* |
| C2B | *Consumer to Business* |
| C2C | *Consumer to Consumer* |
| CAD | Decreto Legislativo 7 marzo 2005, num. 82. Codice dell'amministrazione digitale |
| CC | Real Decreto de 24 de julio de 1889 por el que se publica el Código civil |
| CCLCS | Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la lucha contra el *spam*, los programas espía y los programas maliciosos de 15 de noviembre de 2006 |

| | |
|---|---|
| CCom | Real Decreto de 22 de agosto de 1885 por el que se publica el Código de comercio |
| CE | Constitución Española |
| CERES | Certificación Española |
| CERN | *Conseil Européen pour la Recherche Nucléaire* |
| CGC | Condiciones generales de la contratación |
| CLAOC | Convenio 80/934/CEE sobre la ley aplicable a las obligaciones contractuales abierto a la firma en Roma el 19 de junio de 1980 |
| CNMV | Comisión Nacional del Mercado de Valores |
| CNUCCIM | Comisión de las Naciones Unidas sobre los contratos de compraventa internacional de mercaderías |
| CNUDMI | Comisión de las Naciones Unidas para el Derecho mercantil internacional |
| CNUUCECI | Convención de las Naciones Unidas sobre la utilización de las comunicaciones electrónicas en los contratos internacionales |
| CP | Ley Orgánica 10/1995, de 23 de noviembre, del Código penal |
| CR | Convenio de Roma de 1980 sobre la ley aplicable a las obligaciones contractuales |

**D**

| | |
|---|---|
| D. A. | Disposición/disposiciones adicional/es |
| DAAEDE | Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se modifican las Directivas 2005/60/CE y 2006/48/CE y se deroga la Directiva 2000/46/CE |

| | |
|---|---|
| DAAEDESCE | Directiva 2000/46/CE del Parlamento Europeo y del Consejo de 18 de septiembre de 2000 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio así como la supervisión cautelar de dichas entidades |
| DADDALCP | Directiva 2006/100/CE del Consejo de 20 de noviembre de 2006 por la que se adaptan determinadas directivas en el ámbito de la libre circulación de personas, con motivo de la adhesión de Bulgaria y Rumanía |
| DADLRAEMCC | Directiva 98/7/CE del Parlamento Europeo y del Consejo de 16 de febrero de 1998 que modifica la Directiva 87/102/CEE relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de crédito al consumo |
| DADLRAEMPE | Directiva 84/450/CEE del Consejo de 10 de septiembre de 1984 relativa a la aproximación de las disposiciones legales, reglamentarias y administrativas de los Estados miembros en materia de publicidad engañosa |
| DADPAST | Directiva 2011/24/UE del Parlamento Europeo y del Consejo de 9 de marzo de 2011 relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza |
| DALEMIVN | Sexta Directiva 77/388/CEE del Consejo de 17 de mayo de 1977 en materia de armonización de las legislaciones de los Estados miembros relativas a los impuestos sobre el volumen de negocios – Sistema común del Impuesto sobre el Valor Añadido: base imponible uniforme |
| DAPIC | Directiva 98/27/CE del Parlamento Europeo y del Consejo de 19 de mayo de 1998 relativa a las acciones de cesación en materia de protección de los intereses de los consumidores |

| | |
|---|---|
| DART | Directiva 89/552/CEE del Consejo de 3 de octubre de 1989 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva |
| DCACCC | Directiva 93/13/CEE del Consejo de 5 de abril de 1993 sobre las cláusulas abusivas en los contratos celebrados con consumidores |
| DCDLRADOICVM | Directiva 85/611/CEE del Consejo de 20 de diciembre de 1985 por la que se coordinan las disposiciones legales, reglamentarias y administrativas sobre determinados organismos de inversión colectiva en valores mobiliarios |
| DCDLRASDDSV(I) | Segunda Directiva 88/357/CEE del Consejo de 22 de junio de 1988 sobre coordinación de las disposiciones legales, reglamentarias y administrativas relativas al seguro directo distinto del seguro de vida, por la que se establecen las disposiciones destinadas a facilitar el ejercicio efectivo de la libre prestación de servicios y por la que se modifica la Directiva 73/23/CEE |
| DCDLRASDDSV(II) | Directiva 92/49/CEE del Consejo de 18 de junio de 1992 sobre coordinación de las disposiciones legales, reglamentarias y administrativas relativas al seguro directo distinto del seguro de vida y por la que se modifican las Directivas 73/239/CEE y 88/357/CEE (tercera Directiva de seguros distintos del seguro de vida) |
| DCDLRASDV(I) | Segunda Directiva 90/619/CEE de 8 de noviembre de 1990 sobre la coordinación de las disposiciones legales, reglamentarias y administrativas relativas al seguro directo de vida, por la que se establecen las disposiciones destinadas a facilitar el ejercicio efectivo de la libre prestación de servicios y por la que se modifica la Directiva 79/267/CEE |

| | |
|---|---|
| DCDLRASDV(II) | Directiva 92/96/CEE del Consejo de 10 de noviembre de 1992 sobre coordinación de las disposiciones legales, reglamentarias y administrativas relativas al seguro directo de vida, y por la que se modifican las Directivas 79/267/CEE y 90/619/CEE (tercera Directiva de seguros de vida) |
| DCDSFDC | Directiva 2002/65/CE del Parlamento Europeo y del Consejo de 23 de septiembre de 2002 relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, y por la que se modifican la Directiva 90/619/CEE del Consejo y las Directivas 97/7/CE y 98/27/CE |
| DCE | Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000 relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) |
| DCMO | Decisión 2000/709/CE de la Comisión de 6 de noviembre de 2000 relativa a los criterios mínimos que deben tener en cuenta los Estados miembros para designar organismos de conformidad con el apartado 4 del artículo 3 de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica |
| DCMRI | Decisión 2004/563/CE de la Comisión de 7 de julio de 2004 por la que se modifica su Reglamento interno |
| DCMST | Directiva 90/388/CEE de la Comisión de 28 de junio de 1990 relativa a la competencia en los mercados de servicios de telecomunicaciones |
| D. D. | Disposición/disposiciones derogatoria/s |
| DDC | Directiva 2011/83/UE del Parlamento Europeo y del Consejo de 25 de octubre de 2011 sobre los derechos de los consumidores, por la que se modifican la Directiva 91/13/CEE del Consejo |

| | |
|---|---|
| | y la Directiva 1999/44/CE del Parlamento Europeo y del Consejo y se derogan la Directiva 85/577/CEE del Consejo y la Directiva 97/7/CE del Parlamento Europeo y del Consejo |
| DECFPN | Decisión de ejecución (UE) 2015/1984 de la Comisión de 3 de noviembre de 2015 por la que se definen las circunstancias, formatos y procedimientos de notificación con arreglo al artículo 9, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior |
| DEEFFEASEA | Decisión de ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior |
| DEETFLC | Decisión de ejecución (UE) 2015/1505 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones técnicas y los formatos relacionados con las listas de confianza de conformidad con el artículo 22, apartado 5, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior |
| DEMPCEMMIE | Decisión de ejecución (UE) 2015/296 de la Comisión de 24 de febrero de 2015 por la que se establecen las modalidades de procedimiento para la cooperación entre los Estados miembros en materia de identificación electrónica con arreglo al artículo 12, apartado 7, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo relativo a la identificación electrónica y |

| | |
|---|---|
| | los servicios de confianza para las transacciones electrónicas en el mercado interior |
| DENESDCCFS | Decisión de ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior |
| D. F. | Disposición/disposiciones final/es |
| DFE | Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica |
| DGRN | Dirección General de los Registros y del Notariado |
| DLAPIN | Decreto Legislativo 2 luglio 2010, num. 110. Disposizioni in materia di atto pubblico informatico redatto dal notaio, a norma dell'articolo 65 della Legge 18 giugno 2009, num. 69 |
| DLCAD | Decreto Legislativo 4 aprile 2006, num. 159. Disposizioni integrative e correttive al Decreto Legislativo 7 marzo 2005, num. 82, recante Codice dell'amministrazione digitale |
| DLDFE | Decreto Legislativo 23 gennaio 2002, num. 10. Attuazione della Direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche |
| DLDU | Decreto-legge 25 giugno 2008, num. 112. Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione tributaria |

| | |
|---|---|
| DLMICAD | Decreto Legislativo 30 dicembre 2010, num. 235. Modifiche ed integrazioni al Decreto Legislativo 7 marzo 2005, num. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della Legge 18 giugno 2009, num. 69 |
| DLMU | Decreto-legge 29 novembre 2008, num. 185. Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale |
| DLUM | Decreto-legge 18 ottobre 2012, num. 179. Ulteriori misure urgenti per la crescita del paese |
| DMCAGLIST | Directiva 97/13/CE del Parlamento Europeo y del Consejo de 10 de abril de 1997 relativa a un marco común en materia de autorizaciones generales y licencias individuales en el ámbito de los servicios de telecomunicaciones |
| DMDART | Directiva 97/36/CE del Parlamento Europeo y del Consejo de 30 de junio de 1997 por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva |
| DMDARTP | Directiva 2007/65/CE del Parlamento Europeo y del Consejo de 11 de diciembre de 2007 por la que se modifica la Directiva 89/552/CEE del Consejo sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva |
| DMDPINRT | Directiva 98/48/CE del Parlamento Europeo y del Consejo de 20 de julio de 1998 que modifica la Directiva 98/34/CE por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas |

| | |
|---|---|
| DNCDMISPCMCS | Directiva 97/67/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa a las normas comunes para el desarrollo del mercado interior de los servicios postales de la Comunidad y la mejora de la calidad del servicio |
| DNI | Documento Nacional de Identidad |
| DNIe | Documento Nacional de Identidad electrónico |
| DOCE | Diario Oficial de las Comunidades Europeas |
| DOUE | Diario Oficial de la Unión Europea |
| DPCCD | Directiva 97/7/CE del Parlamento Europeo y del Consejo de 20 de mayo de 1997 relativa a la protección de los consumidores en materia de contratos a distancia |
| DPCD | Directiva 2005/29/CE del Parlamento Europeo y del Consejo de 11 de mayo de 2005 relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) nº 2006/2004 del Parlamento Europeo y del Consejo («Directiva sobre las prácticas comerciales desleales») |
| DPCE | Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) |
| DPCMCAD | Decreto del Presidente del Consiglio dei Ministri 9 febbraio 2011. Modalità, limiti e tempi di applicazione del Codice dell'amministrazione digitale |

| | |
|---|---|
| DPCMDI | Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999. Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, num. 513 |
| DPCMFEA | Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013. Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 |
| DPCMMCAD | Decreto del Presidente del Consiglio dei Ministri 2 marzo 2011. Modalità, limiti e tempi di applicazione delle disposizioni del Codice dell'amministrazione digitale all'agenzia delle entrate |
| DPIMRTRRSSI | Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo de 9 de septiembre de 2015 por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (versión codificada) |
| DPINRT | Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998 por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas |
| DPJBD | Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996 sobre la protección jurídica de las bases de datos |
| DPJTPS | Directiva 87/54/CEE del Consejo de 16 de diciembre de 1986 sobre la protección jurídica de las topografías de los productos semiconductores |

| | |
|---|---|
| DPNRNPFE | Decisión 2003/511/CE de la Comisión de 14 de julio de 2003 relativa a la publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica, de conformidad con lo dispuesto en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo |
| DPPFTDP | Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos |
| DPRAI | Decreto del Presidente della Repubblica 18 agosto 2000, num. 308. Regolamento concernente l'utilizzazione di procedure telematiche per gli adempimenti tributari in materia di atti immobiliari |
| DPRDA | Decreto del Presidente della Repubblica 28 dicembre 2000, num. 445. Disposizioni legislative in materia di documentazione amministrativa (Testo A) |
| DPRDSIT | Decreto del Presidente della Repubblica 10 novembre 1997, num. 513. Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, num. 59 |
| DPRFE | Decreto del Presidente della Repubblica 7 aprile 2003, num. 137. Regolamento recante disposizioni di coordinamento in materia di firme elettroniche a norma dell'articolo 13 del Decreto Legislativo 23 gennaio 2002, num. 10 |
| DRCP | Directiva 2005/36/CE del Parlamento Europeo y del Consejo de 7 de septiembre de 2005 relativa al reconocimiento de cualificaciones profesionales |
| DSGP | Directiva 92/59/CEE del Consejo de 29 de junio de 1992 relativa a la seguridad general de los productos |

| | |
|---|---|
| DSGRTES | Directiva 89/48/CEE del Consejo de 21 de diciembre de 1988 relativa a un sistema general de reconocimiento de los títulos de enseñanza superior que sancionan formaciones profesionales de una duración mínima de tres años |
| DSMI | Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior |
| DSPMI | Directiva 2007/64/CE del Parlamento Europeo y del Consejo de 13 de noviembre de 2007 sobre servicios de pago en el mercado interior, por la que se modifican las Directivas 97/7/CE, 2002/65/CE, 2005/60/CE y 2006/48/CE y por la que se deroga la Directiva 97/5/CE |
| DSSGRFP | Directiva 92/51/CEE del Consejo de 18 de junio de 1992 relativa a un segundo sistema general de reconocimiento de formaciones profesionales, que completa la Directiva 89/48/CEE |
| DSSI | Destinatario/s de servicio/s de la sociedad de la información |
| DSSIi | Destinatario/s de servicio/s de la sociedad de la información de intermediación |
| DSSIic | Destinatario/s de servicio/s de la sociedad de la información de intermediación certificadora |
| DSSIisc | Destinatario/s de servicio/s de la sociedad de la información de intermediación de servicios de confianza |
| D. T. | Disposición/disposiciones transitoria/s |
| DTDP | Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones |

**E**

| | |
|---|---|
| EDI | *Electronic Data Interchange* |
| EEE | Espacio Económico Europeo |
| EFT | *Electronic Funds Transfer* |
| eIDAS | *electronic IDentification Authentication and Signature* |
| ENISA | *European Union Agency for Network and Information Security* |
| eTS | *electronic Trust Services* |

**F**

| | |
|---|---|
| FNC | *Federal Networking Council* |
| FNMT-RCM | Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda |

**H**

| | |
|---|---|
| HTML | *HyperText Markup Language* |
| HTTP | *HyperText Transfer Protocol* |

**I**

| | |
|---|---|
| IADFE | Informe de la Comisión al Parlamento Europeo y al Consejo de 15 de marzo de 2006 sobre la aplicación de la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica |
| IDABC | *Interoperable Delivery of european eGovernment services to public Administrations, Business and Citizens* |
| IP | *Internet Protocol* |
| IRC | *Internet Relay Chat* |
| IVA | Impuesto sobre el Valor Añadido |

## J

| | |
|---|---|
| JACUDI | *JApan Computer Usage Development Institute* |

## L

| | |
|---|---|
| LAICE | Legge 29 dicembre 2000, num. 422. Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità Europee - Legge comunitaria 2000 |
| LANCIDPD | Ley 26/2011, de 1 de agosto, de adaptación normativa a la convención internacional sobre los derechos de las personas con discapacidad |
| LAR | *Local Area Network* |
| LC | Ley 22/2003, de 9 de julio, concursal |
| LCDRCE-RPC | Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones |
| LCDSFDC | Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores |
| LCGC | Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación |
| LDAGOPCM | Legge 23 agosto 1988, num. 400. Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri |
| LEART | Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, sobre la coordinación de disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva |
| LECiv | Ley 1/2000, de 7 de enero, de enjuiciamiento civil |

| | |
|---|---|
| LES | Ley 2/2011, de 4 de marzo, de economía sostenible |
| LFBAPS | Legge 23 dicembre 2009, num. 191. Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato |
| LFE | Ley 59/2003, de 19 de diciembre, de firma electrónica |
| LG | Ley 50/1997, de 27 de noviembre, del Gobierno |
| LGCA | Ley 7/2010, de 31 de marzo, general de la comunicación audiovisual |
| LGDCU | Ley 26/1984, de 19 de julio, general para la defensa de los consumidores y usuarios |
| LGP | Ley 34/1988, de 11 de noviembre, general de publicidad |
| LGT | Ley 9/2014, de 9 de mayo, general de telecomunicaciones |
| LGTr | Ley 58/2003, de 17 de diciembre, general tributaria |
| LH | Decreto de 8 de febrero de 1946 por el que se aprueba la nueva redacción oficial de la Ley Hipotecaria |
| LI | Ley 21/1992, de 16 de julio, de industria |
| LIFE-CRCFSP | Ley 25/2013, de 27 de diciembre, de impulso de la factura electrónica y creación del registro contable de facturas en el sector público |
| LIVA | Ley 37/1992, de 28 de diciembre, del impuesto sobre el valor añadido |
| LJCA | Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa |
| LMACI | Ley Modelo de la CNUDMI sobre arbitraje comercial internacional |
| LMCE | Ley Modelo de la CNUDMI sobre comercio electrónico |

| | |
|---|---|
| LMFE | Ley Modelo de la CNUDMI sobre firmas electrónicas |
| LMISI | Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información |
| LMSO | Ley 25/2015, de 28 de julio, de mecanismo de segunda oportunidad, reducción de la carga financiera y otras medidas de orden social |
| LMTRLGDCU | Ley 3/2014, de 27 de marzo, por la que se modifica el Texto Refundido de la Ley general para la defensa de los consumidores y usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre |
| LMV | Ley 24/1988, de 28 de julio, del mercado de valores |
| LN | Ley del notariado, de 28 de mayo de 1862 |
| LOCM | Ley 7/1996, de 15 de enero, de ordenación del comercio minorista |
| LOMLOPJ | Ley Orgánica 7/2015, de 21 de julio, por la que se modifica la Ley Orgánica 6/1985, del poder judicial |
| LOPDCP | Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal |
| LOPJ | Ley Orgánica 6/1985, de 1 de julio, del poder judicial |
| LOPSC | Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana |
| LOTADCP | Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal |
| LPACAP | Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones públicas |

| | |
|---|---|
| LPASA | Legge 15 marzo 1997, num. 59. Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della pubblica Amministrazione e per la semplificazione amministrativa |
| LPGE | Ley 17/2012, de 27 de diciembre, de presupuestos generales del Estado para el año 2013 |
| LPHE | Ley 16/1985, de 25 de junio, del patrimonio histórico español |
| LRJAP-PAC | Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común |
| LSESCPC | Legge 18 giugno 2009, num. 69. Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile |
| LSSICE | Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico |
| LUMUCP | Legge 17 dicembre 2012, num. 221. conversione, con modificazioni, del Decreto-legge 18 ottobre 2012, num. 179, recante ulteriori misure urgenti per la crescita del paese |

**O**

| | |
|---|---|
| OADPPCMI | ORDEN INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior |
| OMOADPPCMI | Orden INT/665/2015, de 27 de marzo, por la que se modifica la Orden INT/738/2006, de 13 de marzo, por la que se aprueba la declaración de prácticas y políticas de certificación del Ministerio del Interior |

| | |
|---|---|
| ONASFT | Orden de 22 de marzo de marzo de 1996 por la que se dictan las normas de aplicación del sistema de facturación telemática previsto en el artículo 88 de la Ley 37/1992, de 28 de diciembre, del impuesto sobre el valor añadido, y desarrollado en el artículo 9 bis del Real Decreto 2402/1985, de 18 de diciembre |
| OORVPBM | Orden de 19 de julio de 1999 por la que se aprueba la Ordenanza para el registro de venta a plazos de bienes muebles |
| ORAPSSIisc | Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica |
| OTECE | Orden EHA/3256/2004, de 30 de septiembre, por la que se establecen los términos en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 35.4 de la Ley General Tributaria |

**P**

| | |
|---|---|
| P2P | *Peer to Peer* |
| PAFE | Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones de 28 de noviembre de 2008 |
| PDLMICAD | Decreto Legislativo 30 dicembre 2010, num. 235. Modifiche ed integrazioni al Decreto Legislativo 7 marzo 2005, num. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della Legge 18 giugno 2009, num. 69 |
| PDMCSFE | Propuesta de Directiva sobre un marco común para los servicios de firma electrónica |
| PIN | *Personal Identification Number* |
| PKI | *Public Key Infraestructure* |

| | |
|---|---|
| PLMFAOS | Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y de orden social |
| PRDMRDEDNI-CFE | Real Decreto 1586/2009, de 16 de octubre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica |
| PSSI | Prestador/es de servicio/s de la sociedad de la información |
| PSSIi | Prestador/es de servicio/s de la sociedad de la información de intermediación |
| PSSIic | Prestador/es de servicio/s de la sociedad de la información de intermediación certificadora |
| PSSIisc | Prestador/es de servicio/s de la sociedad de la información de intermediación de servicios de confianza |

**R**

| | |
|---|---|
| RACRDLFE | Resolución de 21 de octubre de 1999, del Congreso de los Diputados, por la que se ordena la publicación del acuerdo de convalidación del Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica |
| RAE | Real Academia Española |
| RBIbis | Reglamento (UE) nº 1215/2012 del Parlamento Europeo y del Consejo de 12 de diciembre de 2012 relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil |
| RDCGC | Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de la contratación |

| | |
|---|---|
| RDDEEFIEP | Real Decreto 2402/1985, de 18 de diciembre, por el que se regula el deber de expedir y entregar factura que incumbe a los empresarios y profesionales |
| RDEDNI-CFE | Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica |
| RDLFE | Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica |
| RDRDLOPDCP | Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal |
| RDRDM | Real Decreto 415/2016, de 3 de noviembre, por el que se reestructuran los departamentos ministeriales |
| RDTDMIEGCE | Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista |
| RDTICPTDASC | Resolución de 14 de diciembre de 2015, de la Dirección de Tecnologías de la Información y las Comunicaciones, por la que se establecen las prescripciones técnicas necesarias para el desarrollo y aplicación del sistema Cl@ve |
| RDUTEITAGE | Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado |

| | |
|---|---|
| REERFECUESCC | Reglamento de ejecución (UE) 2015/806 de la Comisión de 22 de mayo de 2015 por el que se establecen especificaciones relativas a la forma de la etiqueta de confianza «UE» para servicios de confianza cualificados |
| REFEPTMNSMIE | Reglamento de ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior |
| REMI | Reglamento de ejecución (UE) 2015/1501 de la Comisión de 8 de septiembre de 2015 sobre el marco de interoperabilidad de conformidad con el artículo 12, apartado 8, del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior |
| RIE-SCTE | Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE |
| RITPAJD | Real Decreto 828/1995, de 29 de mayo, por el que se aprueba el Reglamento del impuesto sobre transmisiones patrimoniales y actos jurídicos documentados |
| RPPFTDP | Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) |

| | |
|---|---|
| RRAVMRCP | Reglamento (CE) nº 765/2008 del Parlamento Europeo y del Consejo de 9 de julio de 2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) nº 339/93 |
| RRI | Reglamento (CE) nº 593/2008 del Parlamento Europeo y del Consejo de 17 de junio de 2008 sobre la ley aplicable a las obligaciones contractuales (Roma I) |

**S**

| | |
|---|---|
| SDLMICAD | Decreto Legislativo 26 agosto 2016, num. 179. Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al Decreto Legislativo 7 marzo 2005, num. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, num. 124, in materia di riorganizzazione delle Amministrazioni pubbliche |
| SIECE | Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo y al Comité de las Regiones |
| SLMFAOS | Ley 24/2001, de 27 de diciembre, de medidas fiscales, administrativas y del orden social |
| SRDMRDEDNI-CFE | Real Decreto 869/2013, de 8 de noviembre, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica |
| SSI | Servicio/s de la sociedad de la información |
| SSIi | Servicio/s de la sociedad de la información de intermediación |
| SSIic | Servicio/s de la sociedad de la información de intermediación certificadora |

| | |
|---|---|
| SSIisc | Servicio/s de la sociedad de la información de intermediación de servicios de confianza |
| STJUE | Sentencia del Tribunal de Justicia de la Unión Europea |
| STS | Sentencia del Tribunal Supremo |

**T**

| | |
|---|---|
| TC | Tribunal Constitucional |
| TCP | *Transmission Control Protocol* |
| TFUE | Tratado de funcionamiento de la Unión Europea |
| TLMFAOS | Ley 53/2002, de 30 de diciembre, de medidas fiscales, administrativas y del orden social |
| TRDMRDEDNI-CFE | Real Decreto 414/2015, de 29 de mayo, por el que se modifica el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica |
| TRLGDCU | Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley general para la defensa de los consumidores y usuarios y otras leyes complementarias |
| TRLMV | Real Decreto Legislativo 4/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del mercado de valores |
| TS | Tribunal Supremo |

**U**

| | |
|---|---|
| UE | Unión Europea |
| UHF | *Ultra High Frequency* |
| UNIDROIT | *Institut international pour l'unification du droit privé* |
| URI | *Uniform Resource Identifier* |

| | |
|---|---|
| URL | *Uniform Resource Locator* |

**V**

| | |
|---|---|
| VHF | *Very High Frequency* |

**W**

| | |
|---|---|
| www | *world wide web* |

# INTRODUZIONE

Il presente lavoro si prefigge come scopo primordiale quello di essere utile a quegli studiosi di Giurisprudenza che intendono approfondire lo studio di una innovativa e, allo stesso tempo, classica istituzione del nostro ordinamento giuridico, nazionale e comunitario. Stiamo parlando della firma elettronica, un'essenziale servizio di fiducia che acquista una rinnovata funzione a seguito dell'entrata in vigore del Regolamento eIDAS e della sua normativa di attuazione, quadro legale fondamentale dal 2006 per l'Unione Europea come conseguenza della deroga effettuata della precedente DFE.

Attualmente ci ritroviamo pertanto, e in un contesto puramente interno, con una situazione paradossale per la vigenza di una norma, la LFE, che, con i risvolti che verranno messe in luce in questo lavoro, ha incorporato nel Diritto spagnolo la Direttiva abrogata, la quale, perciò, avrà bisogno di una trasformazione radicale in modo tale da adattarsi alle esigenze specifiche del nuovo RIE-SCTE. Questa trasformazione, che non è ancora avvenuta in maniera efficace, potrebbe verificarsi tramite due vie differenti: una prima via consiste nella modifica del testo della norma già in vigore affinché sia coerente con la legislazione europea da cui dipende; una seconda via, invece, tende all'abrogazione e alla conseguente introduzione di una nuova legge che, fin dalla sua approvazione, si accordi con il Regolamento e rafforzi tutto ciò che quest'ultimo affida alla competenza propria degli Stati membri. Questa seconda strada è quella che sembra essere stata scelta dal nostro legislatore che, consapevole dello spessore della riforma, ha preferito cominciare già con l'esecuzione di ciò che sembra l'embrione della futura Legge nazionale regolatrice di determinati aspetti dei servizi elettronici di fiducia, una Legge che, fino al momento della sua entrata in vigore, è conosciuta con l'acronimo ALSEC.

In tali circostanze ed essendo, inoltre, consapevoli della mancanza, manifestata nel corso degli anni, di uno studio che affrontasse in maniera chiara gli effetti concreti della firma elettronica nella contrattazione di natura privata che si realizza tramite questo mezzo virtuale, questo lavoro pretende chiarire quello che, in sintesi, potremmo definire come il rapporto

tra il più importante servizio della società dell'informazione e il più rilevante servizio che funge da intermediario. Infatti, sebbene non sia strettamente necessaria per il principio di libertà che regola il nostro Diritto tradizionale, la firma elettronica acquista un nuovo ruolo alla luce delle nuove tecnologie richiedenti nuovi metodi che consentano uno svolgimento sicuro dei rapporti giuridico-economici tra persone fisiche la cui identità, nel nuovo contesto telematico, è reciprocamente sconosciuta.

Questa ricerca consta di quattro capitoli a cui fanno seguito una serie di riflessioni conclusive, accompagnate dalla bibliografia utilizzata, un elenco della giurisprudenza menzionata e, infine, un totale di trenta allegati in cui si presenta in maniera più comprensibile il contenuto di certi aspetti significativi del testo.

Il primo di questi capitoli, intitolato *Nuove tecnologie dell'informazione e della comunicazione: il caso della distanza e del tempo*, affronta la questione relativa al fenomeno della società dell'informazione e al suo veicolo fondamentale: internet. In esso analizzeremo, in primo luogo, l'origine, il significato e l'evoluzione del termine *società dell'informazione*, e il suo passaggio verso la cosiddetta *società della conoscenza*, includendo, al contempo, il discorso filosofico relativo alla configurazione di quello che viene considerato come un nuovo terzo contesto: l'ambito digitale. Verranno presi in esame anche i principali canali che hanno consentito la sua espansione in tutto il pianeta, rappresentati dall'EDI, in un primo stadio, e poi dalla rete globale, omnicomprensiva e tendenzialmente aperta a tutti. Questo progresso avviene in maniera definitiva con la creazione della cosiddetta *www* o *Web*, un nuovo modello di sistema informatico che cambia radicalmente l'idea di internet e che sarà sottoposta a una trasformazione parallela dalla primitiva Web 1.0, senza la compresenza con l'utente e abilitata soltanto per la lettura di contenuti, fino alla nascente Web 4.0, la cui eventuale applicazione avrebbe come scopo principale quello di collegare le persone con i dispositivi affinché entrambi siano in grado di prendere decisioni in maniera congiunta.

Inoltre, per quel che maggiormente ci riguarda, verrà altresì messa a punto una riflessione sulla società dell'informazione come realtà che il Diritto deve cercare di regolare (di solito *a posteriori*, vista la celerità dei progressi tecnologici) per consentire a cittadini e aziende di integrare la Rete nella loro vita quotidiana. A tale scopo, esamineremo, da un lato, la nozione giuridica di SSI come figura globale e la sua distinzione rispetto a quei servizi specializzati d'intermediazione e, dall'altro lato, i soggetti incaricati di fornirli (PSSI e PSSIi) e di utilizzarli

(DSSI e DSSIi). Su questo punto, si rimarca il ruolo della DCE, che cerca di favorire il corretto funzionamento del mercato interno garantendo la libera circolazione dei nuovi servizi sorti nella società dell'informazione e determinate disposizioni nazionali riguardanti comunicazioni commerciali, contratti per via elettronica, codici di condotta, accordi extragiudiziali per la risoluzione delle controversie, ricorsi giurisdizionali e la cooperazione tra i diversi Stati membri. Grazie a tale Direttiva nascerà nel nostro paese la LSSICE che, con maggior sviluppo e profondità, avrà lo scopo di regolare il regime giuridico di tali servizi in relazione alle obbligazioni e al conseguente regime di sanzioni dei soggetti incaricati di fornirli, alla informazione (previa e ulteriore) che devono fornire, alle comunicazioni commerciali virtuali e alla validità ed efficacia dei contratti di natura elettronica.

Per concludere, si farà un esplicito riferimento al sistema, tradizionale in fondo ma innovativo nella forma, del commercio elettronico come elemento principale da cui, come manifestazione esplicita e fondamentale, si realizza la contrattazione virtuale. Su questo punto e sulla sua differenziazione come insieme di dati che, trasmessi tramite i meccanismi forniti dalle nuove tecnologie dell'informazione e della comunicazione, perseguono fini di natura negoziale, cercheremo di offrire un elenco che includa le diverse modalità che può adottare e i vantaggi, i rischi e gli svantaggi che comporta la sua implementazione di fronte al commercio fisico tradizionale.

Il secondo capitolo, intitolato *Validità ed efficacia dei contratti privati conclusi per via elettronica*, esamina la contrattazione elettronica che si svolge tra privati e per la quale, in tale caso, si farà ricorso alla firma elettronica che deve rendere nota la volontà e il consenso dei contraenti per quanto riguarda il proprio contenuto dell'accordo negoziale.

Il capitolo si apre con un innovativo approccio sulla natura giuridica del documento, di cui il contratto elettronico non è altro che una modalità singolare. A tal fine, si partirà da una previa esposizione dello stato della questione, caratterizzata dall'esistenza di due teorie fondamentali: da una parte, *la teoria rigida, dello scritto, ristretta o latina*, che sostiene che il documento deve essere sempre formulato per iscritto su supporto fisico e il supporto fisico su carta, identificando questi termini come sinonimi, e, dall'altra parte, la cosiddetta *teoria della rappresentazione o germanica*, predominante dal momento in cui emergono fortemente i progressi consentiti dal mondo digitale e che tende a negare l'esclusività dello scritto come elemento di definizione del documento, concependolo come un contenuto che offre informa-

zione al di là del supporto fisico e del registro in cui si contiene. Frutto della critica ai fondamenti delle due teorie precedenti, si proporrà una nuova teoria che prende il nome di *teoria del documento come contenuto* e ampliala nozione di quest'ultimo, partendo dalla parola scritta per poi estendersi all'immagine e al suono, che ora potranno essere archiviati per il loro uso posteriore come mezzo di prova in un processo giudiziario. Sulla base di questo rinnovamento teorico, verranno infine evidenziati gli elementi essenziali che il contratto elettronico, in quanto documento, deve possedere oltre alle possibili classificazioni che questo potrebbe assumere a seconda del caso particolare.

Una volta identificate le caratteristiche del documento elettronico, il passo successivo sarà quello di trattare, all'interno della fase negoziale in cui il contratto elettronico si sviluppa come servizio della società dell'informazione, l'attività pubblicitaria da cui solitamente è preceduta. Parleremo, quindi, delle comunicazioni commerciali e dei requisiti che devono concorrere affinché siano valide ed efficaci quando vengono concretizzate nel contesto telematico. Tratteremo, in particolare, di quello che succede in quei casi, piuttosto frequenti, di invio massiccio e indiscriminato di comunicazioni virtuali di tipo pubblicitario o promozionale tramite posta elettronica oppure un altro mezzo equivalente che non siano state richieste previamente o espressamente autorizzate dai destinatari di tali comunicazioni: si tratta del cosiddetto *spamming*. A tal proposito, vedremo che tradizionalmente ci sono state due grandi opzioni in termini di politica legislativa nel momento in cui è stato necessario determinare la liceità o illiceità della posta elettronica indesiderata: una prima opzione raggruppa i cosiddetti sistemi *opt-out*, che permettono di inviare pubblicità indesiderata a tutti i destinatari che non abbiano optato per non riceverla, dovendo dare al destinatario la possibilità di esigere che non gli sia inviata dell'altra pubblicità; e una seconda opzione, quella dei cosiddetti sistemi *opt-in*, dove il messaggio pubblicitario è lecito soltanto se il destinatario ha precedentemente scelto di ricevere comunicazioni commerciali, per cui non è sufficiente non opporsi, ma deve esserci una esplicita richiesta oppure un rifiuto chiaro di invio.

Questa attività previa di tipo pubblicitario o promozionale di cui tratta l'inoltro di comunicazioni commerciali virtuali può (e suole) sfociare nella stipulazione di *contratti telematici* o *contratti stipulati per via elettronica*, intesi come quegli accordi commerciali dove tanto l'offerta come la sua accettazione si trasmettono tramite apparecchiature elettroniche di elaborazione e di memorizzazione di dati collegate a una rete di telecomunicazioni. È per questa ragione che, per questa tipologia di contratti, introdurremo il già citato principio di libertà delle forme: secondo tale principio, quel che davvero importa per poter parlare di un contratto elettronico

valido ed efficace non è la forma in quanto tale, ma l'aspetto consensuale; di conseguenza, da quando c'è consenso (momento controverso come vedremo) esiste il contratto indipendentemente dal registro e dal supporto fisico impiegati dalle parti per esprimerlo. Tuttavia, espliciteremo in maniera chiara la profonda trasformazione che subirà questo principio tradizionale con l'apparizione del Diritto proprio della contrattazione elettronica: in tal senso, mentre il contratto tradizionale per essere valido poteva essere stipulato in maniera scritta oppure orale; quello elettronico, indipendentemente della forma, si deve stipulare, obbligatoriamente, in maniera virtuale, e ciò porta, di conseguenza, a una sorta di limitazione intrinseca, nota come *formalismo indiretto*, che imporrà l'obbligatorietà, più fattuale che giuridica, del supporto.

Per concludere, una parte centrale della nostra ricerca sarà determinata dalla necessità di analizzare quei contratti dotati di firma elettronica come complemento fondamentale a effetto di prova del loro contenuto, della loro attribuzione e integrità. Più specificamente, analizzeremo gli aspetti legislativi generali che regolano questa questione, tanto a livello europeo come a livello interno per la Spagna e l'Italia. A tal proposito, è rimarchevole, per la sua rilevanza e complessità, il contenuto degli allegati XIV e XV, in cui verranno fornite due tabelle comparative di ogni disposizione delle normative comunitarie, spagnola e italiana, prima e dopo la promulgazione e l'entrata in vigore del RIE-SCTE, rispettivamente.

Il terzo capitolo riguarda la *firma elettronica come mezzo di prova dei contratti elettronici privati*.

Questo capitolo si sviluppa a partire da un importante concetto, forse uno dei più importanti che possa chiarire il funzionamento della nuova normativa europea e della firma elettronica come strumento essenziale per creare sufficiente fiducia nell'uso del commercio elettronico: stiamo parlando dei servizi fiduciari digitali. In maniera più specifica, cercheremo di chiarire la loro natura giuridica; è questo un punto controverso per il quale proporremo una teoria (poco conosciuta o, quantomeno, inusuale finora) ignorata addirittura dalla stessa normativa di riferimento, considerato che né la DCE né la LSSICE ne fanno cenno: ci riferiamo all'inclusione dei servizi fiduciari all'interno dei SSIi (da qui si intende il perché li conosciamo con l'acronimo SSIisc) vista la funzione d'intermediazione che svolgono nella prestazione o utilizzazione di SSI e il soddisfacimento di tutti i requisiti (onerosità abituale, distanza, via elettronica e richiesta individuale del DSSI) imposti dalla normativa di riferimento per questo tipo di servizi.

In seguito, un'attenzione speciale sarà riservata ai diversi aspetti generali che distinguono la firma elettronica da qualsiasi altro SSIisc (sigillo elettronico, validazione temporale elettronica, servizio elettronico di recapito certificato e certificato di autenticazione di un sito web). Perciò, oltre all'elenco di firme elettroniche riconosciute legalmente (firma elettronica semplice, firma elettronica avanzata e firma elettronica qualificata), si inquadreranno due elementi essenziali nella conformazione dell'infrastruttura a chiave pubblica di cui godono quelle firme elettroniche che possiedono maggior sicurezza: da un lato, i certificati di firma elettronica rilasciati dai PSSIisc, e dall'altro, i dati di creazione e verifica di firma.

Come è facilmente intuibile, tra le principali funzioni della firma elettronica nel ristretto ambito della contrattazione *online* vi è l'identificazione dei soggetti contraenti, oltre a garantire in maniera probatoria che ognuna delle comunicazioni che circolano virtualmente vengano realizzate in modo integro e volontario e siano accessibili soltanto per i rispettivi emittenti e destinatari. Ebbene, per l'attribuzione di tutti o alcuni degli effetti sopraindicati, si distinguono di solito due aspetti fondamentali riguardanti la validità e l'efficacia della firma elettronica che analizzeremo separatamente nell'ultimo paragrafo di questo capitolo al fine di fornire una migliore comprensione degli stessi: in primo luogo, ci occuperemo degli aspetti materiali, determinati dagli effetti giuridici particolari che prevede la norma per ogni tipo o modalità di firma elettronica; in secondo luogo, esamineremo gli aspetti meramente processuali, che regolano l'*iter* da percorrere qualora la loro autenticità venga impugnata, per i quali prenderemo in considerazione la controversa forza probatoria del documento in cui troviamo la firma elettronica da includere nel caso.

Questa ricerca si conclude con un quarto e ultimo capitolo, intitolato *elementi soggettivi del sistema di firma elettronica*, nel quale si cercherà di chiarire cosa succede con le diverse parti che intervengono nella stipulazione dei contratti firmati in maniera elettronica e che costituiscono la cosiddetta *struttura triangolare*: firmatario, terzo che si fida della firma elettronica e, soprattutto, PSSIisc come terzo generatore di fiducia.

In relazione a quest'ultimo soggetto, e vista la sua importanza per il valido e corretto funzionamento della rete che compone la firma elettronica, analizzeremo la profonda trasformazione che ha comportato la nuova regolamentazione all'interno del suo ambito d'azione e nella sua stessa denominazione. Infatti, con l'entrata in vigore del Regolamento eIDAS, si ampliano le funzioni dei PSSIisc, che ormai non si riducono alla firma elettronica sebbene continuino a costituirne la sua parte più cospicua.

In particolare, esamineremo un aspetto decisivo quale quello riguardante i principi che regolano il funzionamento di questi soggetti, tra cui possiamo evidenziare il principio di applicazione della legge del paese d'origine, il principio del riconoscimento reciproco o di libera prestazione di servizi e il principio di non subordinazione all'autorizzazione preventiva, quest'ultimo particolarmente controverso a causa delle modifiche subite dopo l'entrata in vigore del nuovo Regolamento. Questo lavoro si conclude, infine, con l'analisi degli obblighi che ricadono su questi fornitori e che si riversano in diverse norme, vista la loro eventuale triplice condizione di PSSI, PSSIi e PSSIisc; il conseguente regime di responsabilità a cui verranno sottomessi; l'esigenza, imposta agli Stati membri, di disporre dei necessari mezzi di controllo e indagine per verificare l'adempimento dei PSSI degli obblighi stabiliti normativamente in tutto ciò che riguarda i SSI, e, per ultimo, le concrete e particolari infrazioni e sanzioni che si dovranno imporre ai PSSIisc a seguito dell'inadempimento o esecuzione difettosa degli obblighi imposti.

# CAPÍTULO PRIMERO

# NUEVAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN: EL OCASO DE LA DISTANCIA Y EL TIEMPO

**SUMARIO. - I.** CONSIDERACIONES PRELIMINARES. **II.** LA SOCIEDAD DE LA INFORMACIÓN Y SU DESENVOLVIMIENTO EN EL TERCER ENTORNO. **III.** ORIGEN, SIGNIFICADO Y EVOLUCIÓN DEL TÉRMINO: DE LA *SOCIEDAD DE LA INFORMACIÓN* A LA *SOCIEDAD DEL CONOCIMIENTO*. **IV.** INTERNET COMO FACTOR ESENCIAL DE IMPULSO Y CONSOLIDACIÓN DE LA SOCIEDAD DE LA INFORMACIÓN. **1.** Estadio previo: EDI como paradigma de redes cerradas. **2.** Surgimiento de la red global: una revolución llamada Internet. **3.** Rasgos definitorios del nuevo entorno digital. **4.** Evolución de la tecnología Web. **4.1.** La Web 1.0. **4.2.** La Web 2.0. **4.3.** Hacia las Webs 3.0 y 4.0. **V.** SOCIEDAD DE LA INFORMACIÓN Y DERECHO COMO FENÓMENOS YA INSEPARABLES. **VI.** SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN EN EL ORDENAMIENTO JURÍDICO ESPAÑOL: MARCO NORMATIVO REGULADOR. **1.** Concepto comprensivo de figuras heterogéneas. **2.** Servicios de intermediación. **3.** Prestadores de servicios de la sociedad de la información. **3.1.** Concepto y caracteres. **3.2.** Prestadores de servicios de intermediación. **4.** Destinatarios de servicios de la sociedad de la información. **4.1.** Concepto y caracteres. La figura del consumidor. **4.2.** Destinatarios de servicios de intermediación. **VII.** EL COMERCIO ELECTRÓNICO COMO ESENCIAL SERVICIO DE LA SOCIEDAD DE LA INFORMACIÓN. **1.** Noción. **2.** Posibles clasificaciones. **3.** Ventajas, riesgos e inconvenientes.

## I. CONSIDERACIONES PRELIMINARES

El desarrollo y la difusión exponencial de las nuevas tecnologías de la información y de la comunicación ha incidido en múltiples aspectos de la vida económica, política, cultural y jurídica, redefiniendo los conceptos de espacio, identidad y tiempo y propiciando una evolución en la conformación de la sociedad hacia formas hasta no hace mucho tiempo desconocidas e inimaginables. De manera evidente, este radical avance está favoreciendo un modelo de vida caracterizado, en esencia, por el constante incremento de la comunicación a distancia y la extraordinaria rapidez en la transmisión de la información, protagonista fundamental de

esta nueva etapa que se abre espacio. Experimentamos, de este modo, el tránsito de la vetusta *sociedad industrial* o *postindustrial* a la incipiente *sociedad de la información*[1], nuevo paradigma de carácter socio-tecnológico en el que los bienes más preciados no serán, ya, los materiales.

En esta nueva era de la información, la Red define la morfología social y constituye la base material de los nuevos fenómenos culturales (cultura de la realidad virtual) y económicos (la economía de la información global) que en la colectividad se suceden. Ahora, el poder se extiende, bifurca y desplaza de las instituciones y de las organizaciones hacia los sistemas globales de información, que circulan y mutan en un sistema de geometría variable y geografía desmaterializada[2]. Emerge, en definitiva, una nueva sociedad caracterizada por la centralidad y accesibilidad en masa del saber (proceso que genera, a su vez, una suerte de inteligencia colectiva) y por el predominio de la interacción comunicacional en forma virtual a través de lo que conocemos como *ciberespacio*, *la nueva casa de la mente*[3]. A partir de este momento, como diría LÉVY[4], la técnica propone y el hombre dispone.

---

[1] Y es que, como nítidamente expone SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, Turín, Giappichelli, 2012, p. 1, de la misma manera que la industrialización (el empleo de las máquinas en la elaboración de la materia) supuso el paso de la sociedad agrícola a la sociedad industrial, la informatización (el empleo de las máquinas en la elaboración de la información) está determinando la formación de la *sociedad de la información* o *sociedad informacional.*

[2] CASTELLS OLIVÁN, M., *The power of identity*, Oxford, Wiley-Blackwell, 2010, p. 30.

[3] BARLOW, J. P., «A declaration of the independence of cyberspace», 1996, Davos, Definido por la RAE como «ámbito artificial creado por medios informáticos», este término fue popularizado a raíz de la novela de GIBSON, W., *Neuromancer*, Nueva York, Ace Books, 1984, si bien su origen se encuentra en el relato, también de GIBSON, W., *Johnny Mnemonic*, Nueva York, Ace Books, 1982, incluido en el volumen *Burning Chrome.* Sobre esta cuestión y los aspectos críticos que conlleva su conciliación con el mundo jurídico, *vid.* CABANELLAS DE LAS CUEVAS, G., *Derecho de Internet*, Buenos Aires, Elisa, 2012, pp. 71 a 85, que niega la existencia de un Derecho especial para el ciberespacio, reducido a la existencia de cuestiones jurídicas específicas que deberían ser solucionadas desde la perspectiva de los principios generales en la materia (propiedad intelectual, contratos, etc.) o DI COCCO, C./SARTOR, G., *Temi di Diritto dell'informatica*, Turín, Giappichelli, 2013, p. 1, quienes se hacen eco de la concepción de este mundo virtual como un espacio dotado de cultura y ética propias que, por esa misma razón, no tiene necesidad de política y de Derecho, siendo capaz de autorregularse y de resolver sus propios conflictos con sus propios medios.

[4] LÉVY, P., *Qu'est-ce que le virtuel?*, París, La Découverte, 1998, p. 141.

Las principales ventajas (algunas ya apuntadas) que trae consigo este fenómeno parecen, en la actualidad, evidentes: gracias a él, ciudadanos de todo el mundo pueden acceder desde cualquier punto o terminal y en cualquier momento a información y documentación, actual o pretérita, sita a miles de kilómetros, desde su asiento y sin necesidad de desplazarse, con el consiguiente ahorro temporal y económico que ello supone[5]. Asimismo, se produce una apertura extraordinaria de las posibilidades de comunicación con otras personas e instituciones a escala internacional, sin limitación cuantitativa de ningún tipo, sectorial o espacial[6]. Y todo esto acompañado del nacimiento de novedosas y originales oportunidades de entretenimiento surgidas al albor de esta nueva cultura cibernética[7].

Desde una perspectiva puramente mercantil, la aplicación de estas modernas tecnologías a la actividad económica, más específicamente a aquella que tiene lugar como forma de intermediación entre la producción, de un lado, y el consumo, de otro, origina el nacimiento de una modalidad de comercio, distinto y alternativo (que no incompatible) del comercio

[5] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, Cizur Menor, Aranzadi, 2015, pp. 33 y 34. Conviene precisar, no obstante, el distinto nivel de acceso que a este desarrollo tecnológico se produce entre regiones económicamente más y menos favorecidas, originando una importante discriminación de partida. Así es, la distinta participación en este nuevo modelo social no hace sino acrecentar, en principio, las desigualdades entre *inforricos* (con posibilidades de conexión) e *infopobres* (en situación de desconexión), que hace a algunos autores hablar, incluso, de «apartheid digital»; entre ellos se encuentra MOLINÍ FERNÁNDEZ, F., «Ventajas, inconvenientes e impactos territoriales del comercio electrónico», *Investigaciones geográficas*, vol. 27, 2002, p. 143, quien añade, no obstante, que es muy probable que no haya existido hasta ahora un espacio tan global y con menor discriminación por motivos de raza, nacionalidad, sexo, religión o de cualquier otro tipo. Para un estudio más profundo de esta cuestión, *vid*., entre otros, AMAR RODRÍGUEZ, V. M., «La interculturalidad tecnológica: inforricos e infopobres», en AA.VV. (coord.) *Inmigración, interculturalidad y convivencia*, Ceuta, Instituto de Estudios Ceutíes, 2002,

[6] SANJURJO REBOLLO, B., *Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, protección de datos, negocios audiovisuales, e-commerce, consumidores, marketing*, Madrid, Dykinson, 2015, p. 34.

[7] BRAVO, F., *Contrattazione telematica e contrattazione cibernetica*, Milán, Giuffrè, 2007, p. 625; MIRANDA SERRANO, L. M./VELA TORRES, P. J./PRÍES PICARDO, A., *La contratación mercantil. Disposiciones generales. Protección de los consumidores*, Madrid, Marcial Pons, 2006, p. 336.

tradicional y que ha dado en conocerse como *comercio electrónico*[8]. Los beneficios que se anudan a estos cambios no son tampoco desdeñables, ni por extensión ni por intensidad.

Para el consumidor o usuario, la implementación de este desarrollo tecnológico permite el acceso a un mayor número de bienes y servicios. Ello, unido a la reducción para los productores de aquellos costes derivados de la eliminación de intermediarios[9] y la sustitución de una infraestructura física por una de carácter virtual sin necesidad de almacenamiento material, permite al comprador la obtención de mejores (más baratos) precios, un mayor y más fácil acceso a información relativa a las características de los bienes y servicios ofertados o una mejora en la calidad de los mismos. A ello se añadiría una mayor personalización (las ofertas se encuentran más ajustadas a las necesidades de los clientes), un sustancial incremento del poder negociador merced a la creación de las comunidades virtuales[10] y una minoración, en fin, del tiempo empleado para efectuar la adquisición, al facilitarse la comparación simultánea de precios, condiciones y características.

Para el vendedor o empresario, este traslado del escenario de venta de la calle al ordenador[11] permite saber más acerca de los competidores gracias al aprendizaje organizativo, al

---

[8] *Ibid.*, p. 336.

[9] Con la aparición del comercio electrónico, la importancia de los intermediarios (mayoristas y minoristas) se reduce, ya que se facilita y favorece el contacto entre productores y consumidores. De igual modo, cualquiera de los intermediarios puede relacionarse con el consumidor final, haciendo innecesarios el resto de eslabones de la cadena tradicional. Cierto es, no obstante, que con la aparición y expansión del comercio electrónico también aparecen nuevos intermediarios hasta ahora desconocidos. Para un estudio más profundo de cuanto acabamos de citar, *vid.* GONZÁLEZ SERRANO, L./LAGUNA SÁNCHEZ, P., «Comercio electrónico y empresa: panorama actual y perspectivas futuras», en BOTANA GARCÍA, G. A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 92, 93 y 104.

[10] Las comunidades virtuales hacen referencia a aquellos grupos de personas dotados de cierta estabilidad que se hallan conectados entre sí en línea y someten a discusión uno o varios aspectos cuyo interés es compartido por todos ellos, pudiendo ejercer presión conjunta a fin de alcanzar un objetivo común en materia comercial. De este asunto trata de manera tanto más profunda CARRETERO PÉREZ, J., *Descubre Internet*, Madrid, Prentice Hall, 2001, p. 121 y SÁBADA CHALEZQUER, C., «Interactividad y comunidades virtuales en el entorno de la world wide web», *Comunicación y sociedad*, vol. 1, 2000, pp. 139 a 166.

[11] Varias han sido las respuestas adoptadas frente a este nuevo reto: algunas empresas han optado por la sustitución del establecimiento material tradicional en el que surgieron por un modelo de negocio entera y exclusivamente virtual o telemático. Otras, en cambio, han preferido complementar ambos tipos de mercados, per-

tiempo que posibilita una mayúscula apertura de las oportunidades de negocio, toda vez que los potenciales clientes a los que ahora puede acceder se multiplican de manera extraordinaria. También se favorece una mayor celeridad en el desarrollo de relaciones comerciales y el poder de competir en pie de igualdad con estructuras y organizaciones superiores en tamaño[12].

Ahora bien, como es lógico, nunca todo cambio es enteramente positivo. La inmaterialidad de estos procesos origina desconfianza en el usuario, ávido de una respuesta legal acorde a la trascendencia de los cambios. Así, cuestiones tales como la identificación de la contraparte, la falta de verificación en el momento de efectuar la adquisición del estado y características reales del producto o servicio[13], la incertidumbre acerca de la validez y eficacia de las transacciones que se producen vía electrónica, el desarrollo de prácticas de comercialización no solicitadas y engañosas, el empleo generalizado de los contratos de adhesión, los problemas derivados de la perfección y prueba de los contratos celebrados por este medio, la imposición de cláusulas contractuales abusivas, la posibilidad de tramitar pedidos mediante simple pulsación de teclas, la distribución de riesgos y la delimitación de responsabilidades entre los distintos sujetos intervinientes, el diseño de páginas web que favorecen declaraciones negociales impulsivas[14], la dificultad para determinar la ley y jurisdicción aplicables en caso

maneciendo abiertas al público de un modo físico pero sirviéndose, al mismo tiempo, de estos nuevos instrumentos para potenciar el volumen de sus ventas. Por último, se encuentran aquellas empresas que nacen unidas a esta nueva cultura (las conocidas como empresas *puntocom*).

[12] DÍAZ FRAILE, J. M., «El comercio electrónico: Directiva y Proyecto de Ley español de 2000. Crónica de su contenido, origen, propósitos y proceso de elaboración», *Actualidad civil*, vol. 1, 2001, p. 43; MOLINÍ FERNÁNDEZ, F., «Ventajas, inconvenientes e impactos territoriales del comercio electrónico», cit., pp. 142 a 144; SHAW, M./BLANNING, R./STRADER, T. Y OTROS, *Handbook on Electronic Commerce*, Berlín, Springer, 2000, pp. 19 a 21.

[13] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 33 y 34.

[14] La configuración y el diseño de páginas web dedicadas al negocio con consumidores es fundamental para garantizar la tutela de estos. Para ello, como veremos, es fundamental que se adopten medidas en materia de información, sobre el negocio (identificación, localización, datos de contacto, de registro, códigos de conducta, sistemas de certificación o mecanismos de solución de controversias), sobre las características de los productos y servicios ofertados o sobre las transacciones que tengan lugar (idioma empleado, condiciones generales, coste exacto, condiciones y puesta a disposición, pago, tiempo de entrega, seguridad, servicio postventa, revocación, terminación, derecho de desistimiento o garantías). Además, y para reforzar la decisión consciente del adquirente, es importante que se permita a este, antes de concluir la compra, la posibilidad de identificar con claridad

de litigio como consecuencia de la naturaleza transfronteriza tradicionalmente anudada a este tipo de comercio o la complejidad que supone el acceso en condiciones óptimas de seguridad a servicios en línea públicos y privados, obstaculizan, a menudo, el desarrollo integral de esta nueva modalidad electrónica[15].

## II. LA SOCIEDAD DE LA INFORMACIÓN Y SU DESENVOLVIMIENTO EN EL TERCER ENTORNO

Por encima de toda discusión (aun necesaria) acerca de los beneficios y perjuicios que el ciberespacio supone y conlleva para quienes en él nos hallamos insertos[16], vemos en nuestros días una progresiva adaptación, cuando no directa transformación, de las estructuras sociales tradicionales hacia nuevas formas, irreversibles[17], de vehiculación relacional entre semejantes. La explosiva irrupción de las nuevas tecnologías de la información y de la comunicación[18]

---

los bienes y/o servicios que se desean adquirir, de rectificar el pedido, de manifestar su aceptación final y de obtener un recibo de la operación realizada.

[15] ROSELLO, C., *Commercio elettronico: la governance di Internet tra Diritto statuale, autodisciplina, soft Law e lex mercatoria*, Milán, Giuffrè, 2006, pp. 3 y 4; STOLL, P. T./GOLLER, B., *Electronic commerce and the Internet*, Berlín, German Yearbook of International Law, 1998, p. 162.

[16] Como todo fenómeno, siempre dotado de aspectos favorables y otros no tanto, la aparición del mundo digital no está exenta de críticas. Destáquese entre ellas, a JOYANES AGUILAR, L., *Cibersociedad. Los retos sociales ante un nuevo mundo digital*, Madrid, McGraw-Hill, 1997, p. 256, para quien el cibermundo «no es más que un miserable sustituto de la vida real, en donde reina la frustración y en el que, en nombre de los sagrados principios de la educación y el progreso, aspectos fundamentales de las relaciones humanas son sistemáticamente desvalorizados»; con anterioridad, GUBERN GARRIGA-NOGUES, R., *El simio informatizado*, Milán, Fundesco, 1987, p. 207, consciente de lo inevitable de su llegada, llama a analizar dónde, cómo y cuándo han de aplicarse las nuevas tecnologías, a fin de evitar, en la medida de lo posible, los efectos perniciosos que su uso indiscriminado podría conllevar. Más recientemente y de manera transversal, CARO BEJARANO, M. J., «Peligros tecnológicos», *Cuadernos de estrategia*, vol. 159, 2013, pp. 183 a 227, efectúa, en lo que aquí interesa, un interesante estudio acerca de los riesgos (y posibles medidas preventivas) derivados de un empleo malintencionado o incorrecto de las incesantes innovaciones que se producen en el terreno tecnológico, de la información y de la comunicación.

[17] CLARIZIA, R., *I contratti informatici*, Milanofiori Assago, Utet Giuridica, 2007, p. 3.

[18] Conviene tener en cuenta, como bien apunta PEÑA LÓPEZ, I., «Fundamentos tecnológicos del Derecho de la sociedad de la información», en PEGUERA POCH, M. (coord.) *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010, pp. 52 y 53, que el adjetivo *nuevas* no viene referido tanto al hecho de que estas tecnologías sean más o menos recientes o coetáneas, sino a su contraposición a otras tecnologías de la información y la comunicación. De este modo, el autor realiza una distinción entre antiguas tecnologías de la información y la comunicación, basadas en una representación analógica de la realidad (radio, televisión –VHF,

determina el nacimiento de un nuevo modelo de sociedad que, a diferencia del anterior, otorga palmaria preeminencia económico-social a un elemento inmaterial, pero de fuerza, por su constante celeridad, desconocida: la información, generando una situación verdaderamente expectante y necesitada de acomode.

Aplicado al campo jurídico, los progresos tecnológicos discurren a una velocidad notoriamente superior a la capacidad de adaptación de las viejas estructuras, siempre a remolque. Nace, de este modo, todo un abanico de problemas e incógnitas que requieren de la configuración de mecanismos ágiles capaces de dotar a quienes de este entorno participan (profesionales del Derecho, empresarios, profesionales, consumidores y usuarios) de la confianza y seguridad necesarias para permitir el desenvolvimiento adecuado de los avances de forma tal que impidan su ralentización o interrupción[19].

Comienza, desde entonces, a no contar ni el espacio ni el tiempo, adentrándonos en un proceso de cambio que, superando las etapas correspondientes a la sociedad industrial y postindustrial, concluye con el tránsito hacia lo que comúnmente conocemos como *sociedad de la información*, propiciada por la llamada *Revolución tecnológica* y auspiciada (como tendremos ocasión de ver) por Internet. Esta nueva etapa, también conocida como *era digital* o *sociedad en red* (*network society*), se fundamenta en los avances y convergencia operados en los sectores de las telecomunicaciones y de la informática para configurar un nuevo modelo de desarrollo

UHF–, telefonía fija, prensa escrita, telégrafo, correo o cine), y nuevas tecnologías de la información y la comunicación, fundamentadas en tecnología digital (Internet, telefonía móvil, televisión digital, *world wide web*, redes P2P y LAN, correo electrónico, videoconferencia, voz por IP o mensajería instantánea). A la vista de lo anterior, afirma que «la facilidad con la que estas nuevas tecnologías permiten manejar la información cambia para siempre la forma en que el hombre utiliza los datos, la información o el conocimiento en sus procesos productivos. En primer lugar, el coste de almacenamiento de la información se abarata hasta límites insospechados. En segundo lugar, la velocidad con la que puede transmitirse dicha información a cualquier otro agente se torna prácticamente instantánea. Si a este último factor añadimos el también bajo coste de la transmisión, nos encontramos con que la información puede almacenarse y transmitirse a bajo coste a cualquier punto del planeta y de forma inmediata, pudiendo integrarse en los procesos productivos de una forma mucho más intensiva que hasta el momento».

[19] DAVARA RODRÍGUEZ, M. Á., «La liberalización del mercado de las telecomunicaciones: una perspectiva desde la ética», en PINTO MONTEIRO, A. (coord.) *As telecomunicaçoes e o Direito na sociedade da Informaçao*, Coimbra, Instituto jurídico da comunicaçao, Faculdade de Direito, Universidade de Coimbra, 1999, p. 181.

económico y social que, basado en el predominio de la información como elemento intangible con valor propio y prevalente, hace de la interacción virtual el motor su funcionamiento y desarrollo[20], a veces irreflexivo por la inmediatez de los cambios[21] pero, en cualquier caso, sin precedentes.

Esta nueva sociedad que se abre paso se halla inserta, a su vez, dentro de lo que algunos autores han dado en llamar como la *tercera revolución industrial*[22] o el *tercer entorno*[23], distinguiéndolo de los dos espacios clásicos (natural y urbano, este último de mayor relevancia, al menos en los países más desarrollados) en los que los seres humanos interactúan, en los que influye por medio del fenómeno de la *globalización*, entendida como el surgimiento (cuyo origen se remonta al siglo XV, con el comienzo de la política imperialista española iniciada por los Reyes Católicos) de procesos y sistemas de relaciones sociales multidimensionales y complejas que, no fundados en el sistema de Estado-nación, se caracterizan por propiciar una «convergencia de los Estados del mundo»[24], o, lo que es lo mismo, por una interconexión creciente de la vida económica y cultural entre partes distantes en el mundo[25], fundiéndose con

---

[20] MENÉNDEZ MATO, J. C./GAYO SANTA CECILIA, M. E., *Derecho e informática: ética y legislación*, Vallirana, Bosch, 2014, pp. 66 y 67; SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., p. 3.

[21] Y es que, como subraya VEGA CLEMENTE, V., «Comercio electrónico y reactivación económica», *Revista de estudios económicos y empresariales*, vol. 26, 2014, p. 179, «[l]a inmediatez del cambio […] impide reflexionar con la objetividad y el distanciamiento necesarios de toda investigación sobre las consecuencias de la convergencia de tecnologías».

[22] SMITH, B., «The third industrial revolution: Law and policy for the Internet», *Collected courses of the hague academy of international Law*, vol. 282, 2000, pp. 1 a 45.

[23] ECHEVERRÍA EZPONDA, J., *Los señores del aire: telépolis y el tercer entorno*, Barcelona, Destino, 1999, pp. 1 y ss.

[24] LEVITT, T., «Globalization of markets», *Harvard business review*, vol. 3, 1983, p. 95.

[25] GRAY, J., *False dawn: The delusions of global capitalism*, Nueva York, The New Press, 2000, p. 41. Una de las primeras descripciones del término *globalización* la encontramos en BOBBIO, N., *Diccionario de política*, México D. F., Sigo XXI, 1976, p. 1544, quien expone una tesis sobre el fenómeno que ya, por entonces, comenzaba a vislumbrarse, en los siguientes términos: «[e]l camino a una colaboración internacional cada vez más estrecha ha comenzado a corroer los tradicionales poderes de los Estados soberanos. Influyen mayormente las llamadas comunidades supranacionales que intentan limitar fuertemente la soberanía interior y exterior de los Estados miembros; las autoridades "supranacionales" tienen la posibilidad de asegurar y afirmar por medio de cortes de justicia adecuadas la manera en que su Derecho "supranacional" debe ser aplicado por los Estados a casos

el espacio físico y proporcionando el sustrato para un nuevo tipo de organización social, la sociedad de la información[26]. Siguiendo esta teoría, la construcción del tercer entorno y la emergencia de una metafórica ciudad global (Telépolis, que se superpone a los pueblos, ciudades y estados clásicos encarnados en los dos entornos anteriores, a veces en conflicto con ellos), rompe con la tradicional topología basada en las fronteras y en la proximidad espacio-temporal como modo de generación de las diversas formas sociales para instituir un, hasta ahora desconocido, modelo integral de carácter tecnológico, reticular, asincrónico, multidireccional, transterritorial y transtemporal de interacción a distancia[27].

No siendo una ciudad habitable (los ciudadanos seguirán viviendo en los dos primeros entornos), en ella, sin embargo, se desarrollará (si bien con desigual reparto, en lo que se conoce como *brecha digital*[28]) un porcentaje creciente de la vida social, en particular de la actividad productiva y de consumo, articulada esta a través de las infraestructuras, nacional y

concretos: ha desaparecido el poder de imponer impuestos y comienza a ser limitado el de acuñar moneda […]. Pero hay también nuevos espacios, ya no controlados por el Estado soberano: el mercado mundial ha permitido la formación de empresas multinacionales que tienen poder de decisión no sujeto a nadie y libres de cualquier control […]. Los nuevos medios de comunicación de masas han permitido la formación de una opinión pública mundial […]. La plenitud del poder estatal está en decadencia. Con esto, sin embargo, no desaparece el poder; desaparece solamente una determinada forma de organización del poder, que tuvo su punto de fuerza en el concepto político-jurídico de soberanía». Por su parte, PAMBOUKIS, C., «Droit international privé holistique: droit uniforme et droit international privé», *Recueil des cours*, vol. 330, 2007, pp. 417 a 428, establece un elenco, ciertamente genérico, de los principales cambios propiciados por la globalización, a saber: transformación del modelo de decisión (la llamada *nueva gobernanza*) y alteración del concepto de soberanía, cambio significativo del modelo de producción y distribución de bienes y servicios, modificación del modelo de conocimiento, cambio en la organización social, mutación del concepto de *frontera* y de la división tradicional interna e internacional, interdependencia de las relaciones sociales y transformación de la noción de identidad.

[26] SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., p. 201.

[27] Para una primera visión de esta propuesta, *vid.* ECHEVERRÍA EZPONDA, J., «21 tesis sobre el tercer entorno, Telépolis y la vida cotidiana», *XIV Congreso de estudios vascos*, vol. 14, 1998, pp. 7 a 11. Esta tesis del tercer entorno generaliza la idea tradicional del *entorno telemático* y de los *entornos electrónicos*, expuesta por DYSON, E./GILDER, G./KEYWORTH, G. Y OTROS, «Cyberspace and the american dream: a magna carta for the knowledge age», *The information society*, vol. 12, pp. 295 a 308.

[28] Este término, posiblemente acuñado durante la primera presidencia de Bill Clinton (1993 a 1997), vino a poner de manifiesto que, efectivamente, había quien estaba preparado para la sociedad de la información y quien lo estaba menos o no lo estaba en absoluto. Aunque en el momento inicial de su empleo, el término se

mundial, de la información, origen de la sociedad a la que da nombre. Esta incipiente modalidad de interacción social (pública y privada, generadora de valor añadido propio), cuya calle principal es Internet, modifica profundamente manifestaciones tradicionales varias de las relaciones entre individuos, como pueden ser la política, la ciencia, la educación, el arte, el comercio o el Derecho, protagonistas, estos dos últimos en su conjunción, del análisis del presente estudio, centrado en el comercio electrónico, en la contratación electrónica como manifestación esencial del mismo y en la firma electrónica como medio de generación de confianza en el desenvolvimiento de las relaciones negociales a que aquellos dan lugar.

## III. ORIGEN, SIGNIFICADO Y EVOLUCIÓN DEL TÉRMINO: DE LA *SOCIEDAD DE LA INFORMACIÓN* A LA *SOCIEDAD DEL CONOCIMIENTO*

El término *sociedad de la información*, contrariamente a lo que pueda pensarse, surge en Japón durante la crisis de finales de los años 60, donde se lleva a cabo un estudio acerca del valor económico de la información desarrollado por la organización no lucrativa *JACUDI*, que, a partir de un informe del Ministerio de Industria y Comercio, elabora en 1969 el intitulado *Plan para la sociedad de la información – Un objetivo nacional para el año 2000*, conocido universalmente como *Plan JACUDI*[29]. El presidente de este instituto, Yoneji Masuda, publica en 1980

---

refería únicamente a determinadas clases norteamericanas que corrían el riesgo de quedar excluidas de la sociedad digital, en la actualidad, por *brecha digital* se hace referencia a cualquier clase, sociedad o país que, por algún motivo (cultural, económico, social), tiene dificultades para acceder a algún ámbito de esta nueva sociedad (para una breve historia del término, *vid.* SARTORI, L., *Il divario digitale: Internet e le nuove disuguaglianze social*, Bolonia, Il Mulino, 2006, pp. 1 a 201). Para poder superar esta brecha, se han de implementar acciones de *e-inclusión*, que, como su propio nombre indica, pretenden evitar la exclusión en el mundo en red (*vid.* DÍAZ DUMONT, J. R., *Tecnologías de información y comunicación e inclusión social: estudio científico*, Múnich, Grin, 2015, p. 6). Surge entonces el término anglosajón *e-readiness*, que podría definirse como la capacidad o predisposición para utilizar las nuevas tecnologías de la información y de la comunicación en orden a desarrollar la economía y promover el desarrollo de un país o región; cómo estar, en definitiva, preparado para el mundo en red (HARVARD UNIVERSITY, *Readiness for the networked world: a guide for developing countries*, Cambridge, Center for international development at Harvard University, 2000, p. 3). Estos tres términos (*brecha digital*, *e-inclusión* y *e-readiness*) y las soluciones propuestas en relación a los mismos son, en definitiva, distintos caminos que conducen a un mismo objetivo común: permitir el desarrollo de la sociedad de la información.

[29] Con anterioridad, no obstante, MACHLUP, F., *The production and distribution of knowledge in the United States*, Princeton, Princeton University Press, 1962, define el concepto de *industria del conocimiento* y y explora este como un recurso económico. Paralelamente, MCLUHAN, M., *The Gutenberg galaxy: the making of typographic man*, Toronto, University of Toronto Press, 1962, acuña el término *aldea global* para describir la interconectividad humana a

su libro *The information society as a post-industrial society*[30], que, no sólo populariza la expresión, sino que sirve de base para los planes estratégicos actualmente vigentes. En concreto, este autor define esta nueva sociedad como aquella «que crece y se desarrolla alrededor de la información y aporta un florecimiento general de la creatividad intelectual humana, en lugar de un aumento del consumo material», destacando, como factores claves, el conocimiento y la innovación, junto a la adopción y difusión de las tecnologías que facilitan el tratamiento y transmisión de la información[31]. Estamos, pues, en presencia de un concepto en continua evolución y de naturaleza no estrictamente jurídica, caracterizado por una ausencia de uniformidad terminológica que, a menudo, dificultará su sintetización.

En Europa, el proyecto europeo sobre sociedad de la información, que parte del conocido como *Informe Bangemann*[32], nace como respuesta a la iniciativa estadounidense publicada en 1993, titulada *The national information infrastructure: agenda for action*, que surge como respuesta a las declaraciones efectuadas por el entonces vicepresidente de los Estados Unidos, Al Gore. Este plan de acción europeo parte de la conjunción de fuerzas de los sectores público y privado para, centrándose en tres frentes de acción estrechamente relacionados entre sí, configurar una noción integral de sociedad de la información que abarque distintos fines, esferas y actividades. Estos frentes consistirán, de forma resumida, en evitar el rechazo que puedan suponer las nuevas tecnologías por parte de una población aún no adaptada a su uso, lo que

escala global generada merced a los medios electrónicos de comunicación, afirmando que el desarrollo tecnológico incipiente tiene su reflejo tanto en la organización cognitiva como en la social. Años después, TOURAINE, A., *La société post-industrielle: naissance d'une société*, París, Denoël, 1969, analiza el fenómeno socioeconómico evolutivo de la sociedad, para lo cual utiliza la categoría de *post-industrialismo* a fin de indicar que una nueva era se aproxima, etapa en la que identifica al conocimiento como centro del progreso. Por su parte, BELL, D., *The coming of post-industrial society: a venture in social forecasting*, Nueva York, Basic Books, 1976, sitúa como eje principal al conocimiento teórico, advirtiendo (a modo de vaticinio) que los servicios basados en el conocimiento han de convertirse en la estructura central de la nueva economía y de una sociedad regida por la información. Por último, PORAT, M. U., *The information economy*, Michigan, University of Michigan Library, 1977, que delimita un nuevo campo de la actividad productiva, la *economía de la información*, unida al desarrollo de las nuevas tecnologías.

[30] MASUDA, Y., *The information society as post-industrial society*, New Brunswick, Transaction Publishers, 1980, pp. 1 y ss.

[31] *Ibid.*, p. 3.

[32] COMISIÓN EUROPEA, *Europa y la sociedad global de la información. Recomendaciones al Consejo Europeo*, Bruselas, 1994, pp. 1 a 32.

se tratará de conseguir por medio del control de los riesgos que pueda conllevar; en garantizar un acceso equitativo a la infraestructura y a la prestación de un servicio universal asentado en la evolución tecnológica, y en fomentar y difundir las múltiples ventajas y beneficios que la nueva *cultura de la información* comporta en distintos ámbitos de la sociedad.

Este contexto, caracterizado por la desmaterialización de la información, da paso posteriormente al surgimiento de los modernos medios de comunicación asentados en redes digitales (en particular, Internet), que posibilitan un acceso ilimitado, internacional, abierto e instantáneo a los datos procesados. Y de ahí se pasa al momento actual, en el que los propios sujetos destinatarios de la información, de forma autosuficiente, seleccionan y asimilan internamente el inmenso conjunto de contenidos disponibles a distancia para, fruto del pensamiento autónomo y reflexivo, convertirlos en conocimiento. Esta evolución descrita ha llevado a algunos autores a efectuar una distinción terminológica entre *sociedad de la información* y *sociedad del conocimiento*, término, este último, acuñado por primera vez por Peter Drucker[33]. Así, partiendo de una misma realidad, la sociedad de la información engloba a la sociedad del conocimiento, en forma tal que, mientras que la primera consiste en poner a disposición de la población el acceso a una información cuantitativamente ilimitada (perspectiva externa u objetiva), la segunda, representando un estadio superior de la revolución tecnológica actual, se circunscribe al aprovechamiento o tratamiento racional que de la misma obtenga el individuo (perspectiva interna o subjetiva)[34]. En cualquier caso, la tecnología no define, por sí misma, la sociedad de la información ni la sociedad del conocimiento, (ya hubo tecnología en la etapa de la revolución industrial); lo específico del proceso actual es la vinculación entre las nuevas tecnologías con la información y el conocimiento, erigiéndose estos últimos en los verdaderos protagonistas del cambio[35].

---

[33] DRUCKER, P., *The age of discontinuity: guidelines to our changing society*, Nueva York, Harper & Row, 1969, pp. 1 a 380. Este autor acuña también el término *trabajador del conocimiento*, centrándose en generar una teoría económica encaminada a situar al conocimiento en el centro de la producción de la riqueza, de modo que lo que importa no es la cantidad de información, sino la productividad que se deriva de su transformación en conocimiento (*aprender a aprender*).

[34] MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., p. 76.

[35] Autores como MADRID PARRA, A., «Contratos electrónicos y contratos informáticos», *Revista de la contratación electrónica*, vol. 111, 2011, p. 3, opinan, no obstante, que, en la revolución tecnológica actual, lo característico no

Todo ello permitió afirmar que este modelo de sociedad, más que un proyecto definido, era una aspiración, la del nuevo entorno humano, donde la información, su creación y propagación son el elemento definitorio de las relaciones, individuales y horizontales, entre los individuos[36]. Esta visión se mantiene en la actualidad, si bien, con las precisiones anotadas, se perfecciona, ubicándonos en un momento donde la adquisición, almacenamiento, procesamiento, evaluación, transmisión, distribución y diseminación de la información con vistas a la creación de conocimiento y a la satisfacción de las necesidades de las personas y de las organizaciones juega un papel central en la creación de riqueza y en la definición de la calidad de vida y de las prácticas culturales de los ciudadanos[37].

Podemos afirmar, en definitiva, que comienza un período histórico basado en el predominio del conocimiento y en el esfuerzo por convertir la información en eso mismo, conocimiento[38], dando lugar a un nuevo sistema de carácter tecnológico, en el que el incremento de la productividad no depende del incremento cuantitativo de los factores de producción (capital, trabajo, recursos naturales), sino de la aplicación de la información y sus resultados en la gestión, producción y distribución[39].

---

es el predominio de la información o del conocimiento, sino la aplicación de los mismos a aparatos de procesamiento de la información y de generación de conocimiento, en un círculo de retro alimentación acumulativo entre la innovación y sus usos; no se trataría, pues, de información o conocimiento para actuar sobre la tecnología, como sucedió en las revoluciones tecnológicas anteriores, sino de tecnologías para para actuar sobre la información o conocimiento. Para otros, en cambio, lo característico de la sociedad de la información y del conocimiento es el uso intensivo que de ambas se hace, de tal forma que, por primera vez, devienen tan importantes que nace un sector que, exclusivamente, se dedica a su estudio (PEÑA LÓPEZ, I., «Fundamentos tecnológicos del Derecho de la sociedad de la información», cit., p. 53).

[36] TREJO DELARBRE, R., *La nueva alfombra mágica: usos y mitos de Internet*, Madrid, Fundesco, 1996, p. 25.

[37] PÉREZ PEREIRA, M., *Firma electrónica: contratos y responsabilidad civil*, Cizur Menor, Aranzadi, 2009, p. 25.

[38] LINARES LÓPEZ, J./ORTIZ CHAPARRO, F., *Autopistas inteligentes*, Madrid, Fundesco, 1996, p. 73.

[39] CASTELLS OLIVÁN, M., *La era de la información: economía, sociedad y cultura*, Madrid, Alianza, 1997, p. 47. Estamos, en palabras de este autor (*Ibid.*, p. 51), en presencia de lo que se conoce como *sociedad informacional*, en la que, más allá de si el énfasis está en la información (sociedad de la información) o en el conocimiento (sociedad del conocimiento), lo importante es que una u otra son el ese eje que vertebra la sociedad de una forma mucho más profunda que su simple utilización, acabando por determinar todos o casi todos los aspectos de la vida. Así, el término *informacional* «indica el atributo de una forma específica de organización social en la que la generación, el procesamiento y la transmisión de la información se convierten en las fuentes fundamentales de la

## IV. INTERNET COMO FACTOR ESENCIAL DE IMPULSO Y CONSOLIDACIÓN DE LA SOCIEDAD DE LA INFORMACIÓN

Las tecnologías informáticas han conformado la base para la más grande invención de los últimos decenios, aquella que señala el tránsito al nuevo milenio: Internet. En palabras de SARTOR[40]:

> «[…] si es verdad que el punto de partida de la humanidad es único (todos descendemos de una única población, que habitaba en África hace más de 500 millones de años) y que las migraciones han conducido con posterioridad a la dispersión de los seres humanos a cada una de las zonas habitables del planeta y, por tanto, a su división en grupos distintos, Internet marca de alguna manera la vuelta a la unidad originaria, la posibilidad de cada uno de compartir conocimientos y experiencias con la humanidad entera. Internet representa, pues, un punto de llegada en la historia de la humanidad, que nos abre a un futuro caracterizado por graves riesgos pero, también y sobre todo, por grandes oportunidades».

Conscientes de la relevancia del proceso, en las páginas siguientes analizamos las principales características de Internet, así como su evolución y estado actual.

### 1. Estadio previo: EDI como paradigma de redes cerradas

Un primer momento de desarrollo de la sociedad de la información y del conjunto de servicios que lo integran y conforman se produce a través de redes cerradas, como es el caso de la red EDI, que, aplicándose fundamentalmente al desarrollo de actividades de índole comercial, a él únicamente tienen acceso los usuarios (en general, entidades mercantiles o de crédito de grandes dimensiones, dados los elevados costes que conlleva su utilización) autorizados por las empresas de telecomunicación[41]. Legalmente definido en el artículo 2.b)

---

productividad y el poder, debido a las nuevas condiciones tecnológicas que surgen en este período histórico». También sobre esta cuestión, *vid.* ALFONSO SÁNCHEZ, I. R., «La sociedad de la información, sociedad del conocimiento y sociedad del aprendizaje. Referentes en torno a su formación», *Bibliotecas. Anales de investigación*, vol. 2, 2016, pp. 235 a 243; HEIDENREICH, M., «Die debatte um die wissensgesellschaft», en BÖSCHEN, S./SCHULZ-SCHAEFFER, I. (coords.) *Wissenschaft in der wissensgeseelschaft*, Opladen, Westdeutscher Verlag, 2003, pp. 2 a 25; MUNAR BERNAT, P. A., «Protección de datos en el comercio electrónico», en BOTANA GARCÍA, G. A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, Wolters Kluwer, 2001, pp. 275 a 278.

[40] SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., p. 199.

[41] VEGA CLEMENTE, V., «Comercio electrónico y reactivación económica», cit., pp. 177 y 178.

LMCE[42] como «transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto», este acuerdo de intercambio electrónico de datos consiste en la creación de plataformas tecnológicas que, basadas en relaciones de mutua confianza y desarrolladas a menudo en el mismo sector de actividad[43], permiten la reducción de costes, el desarrollo de acuerdos de suministro conjunto prolongado y el incremento del número de transacciones entre los participantes (intercambio de datos, órdenes comerciales o realización de contratos de aprovisionamiento)[44]. Para posibilitar el funcionamiento del EDI, es necesario que la información transmitida esté estructurada conforme a las normas técnicas de estructuración[45] convenidas entre los participantes, de modo que, en el momento de configurar el mensaje de datos[46], la libertad

[42] Esta norma (A/RES/51/162) forma parte de un conjunto normativo de carácter supraestatal conocido como *soft Law*. Con este término nos referimos a aquellas normas no vinculantes, pero tampoco irrelevantes en términos jurídicos, que proponen soluciones, basadas en la práctica, a problemas particularmente frecuentes en la comunidad internacional y que responden a la exigencia de certeza del Derecho.

[43] NORTON, J. J./REED, C./WALDEN, I., *Cross-border electronic banking: challenges and opportunities*, Londres, Lloyd's, 1995, pp. 55 a 80.

[44] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 26. Sobre las implicaciones jurídicas del EDI, *vid.* FADDA, S., «L'Electronic Data Interchange nella normativa italiana e straniera», *Rivista dell'informazione e dell'informatica*, vol. 1, 1994, pp. 91 y ss.

[45] Por *norma técnica de estructuración*, siguiendo a ILLESCAS ORTIZ, R./PERALES VISCASILLAS, P., *Derecho mercantil internacional. El Derecho uniforme*, Madrid, Centro de estudios Ramón Areces, 2003, pp. 336 y 337, podemos entender los «[…] modos y criterios en virtud de los cuales se configuran los mensajes de datos que circulan entre ordenadores o sistemas de información y que transmiten voluntades negociales o prenegociales de quienes son sus emisores y destinatarios». El correo electrónico es el que mayor libertad otorga a los contratantes en orden a configurar su mensaje, el EDI es el que menor libertad otorga, el SWIFT es uno de los más conocidos exponentes del EDI o el PDF, que ha venido adquiriendo creciente predicamento y uso como norma técnica de estructuración que permite reproducciones intangibles de texto dotadas de todo lujo de detalle figurativo.

[46] Por *mensaje de datos*, de acuerdo a la definición proporcionada por el artículo 7.4 LMACI (A/40/17), más tarde recogido por el artículo 2.a) LMCE, se entiende aquella información que es generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares (término, este último, que denota la noción de *equivalente funcional*, tal y como precisa el apartado 31 de la Guía para la incorporación al Derecho interno de la LMCE), como pudieran ser, a título de ejemplo, el EDI, el correo electrónico, el telegrama, el télex o el telefax. Más tarde, la LMFE (A/RES/56/80) se pronunciará en idénticos términos en su artículo 2.c). Será frecuente que esta información circule, que parta de un iniciador hacia un destinatario, pero no necesariamente tiene que ser transmitida, ya que puede ser sólo archivada o simplemente generada, quedando incluidos todos

de las partes se reduce a completar los espacios en blanco del mensaje predeterminado conforme a dichas normas[47]. Como fácilmente puede intuirse, el factor técnico es clave en la configuración de la estructura en que el EDI se desenvuelve, ya que permite que el mensaje de datos se emita uniforme, normalizado y con información estructurada en la forma antes señalada, permitiendo que sea procesada por el ordenador receptor[48]. Con carácter previo, es necesario que las empresas participantes suscriban acuerdos encaminados a garantizar la efectividad de las transmisiones y el reconocimiento recíproco de su carácter vinculante[49]; de este modo, el EDI habrá de ser diferenciado de los acuerdos (normalmente, de naturaleza contractual) que puedan alcanzarse, a su amparo, con posterioridad[50].

Con frecuencia, los acuerdos EDI se concluyen siguiendo alguno de los modelos elaborados por distintos organismos. Entre ellos, cabe destacar el contenido en el Modelo europeo de acuerdo EDI, que constituye el anexo I de la Recomendación 94/820/CE de la Comisión de 19 de octubre de 1994 relativa a los aspectos jurídicos del intercambio electrónico de

---

estos supuestos. Como acertadamente señala MADRID PARRA, A., «Instrumentos de la CNUDMI/UNCITRAL sobre comercio electrónico (contratación, firma y comunicaciones comerciales)», en PLAZA PENADÉS, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, pp. 311 y 312, en torno a este concepto se construye toda la estructura de la LMCE, empleando, para ello, una formulación absolutamente abierta, de forma que quedan incluidos tanto los medios tecnológicos conocidos en el presente como otros que, sucesivamente, se vayan descubriendo e implementando en el futuro. A tal fin, se recurre a la institución jurídica de la analogía (*principio de neutralidad tecnológica*), de manera que se mencionan medios conocidos en el momento presente, pero como mención en un listado abierto, más a título de ejemplo que de lista cerrada, de modo que puedan quedar incluidos nuevos desarrollos técnicos, como pudieran ser, por ejemplo, los que se generen en el campo de la física cuántica. En el objetivo de la LMCE está, por tanto, todo supuesto de información en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica dentro del ámbito comercial. Este mismo autor (*Ibid.*, p. 310) sostiene que, quizás, la expresión en español *mensaje de datos* no enfatice suficientemente lo más relevante, como es que la información se encuentra en un soporte físico distinto del papel. Por ello, entiende que otras expresiones, pese a presentar también inconvenientes, expondrían mejor esta nota diferencial, como sucedería con los términos *mensaje electrónico*, *archivo electrónico*, *registro electrónico*, *información electrónica* o *datos electrónicos*.

[47] ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, Cizur Menor, Aranzadi, 2009, pp. 75 a 77.

[48] BARRIUSO RUIZ, C., *La contratación electrónica*, Madrid, Dykinson, 1998, pp. 205 a 216.

[49] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 28.

[50] JULIÀ BARCELÓ, R., *Comercio electrónico entre empresarios: la formación y prueba del contrato electrónico (EDI)*, Valencia, Tirant lo Blanch, 2000, pp. 109 a 119.

datos[51]. El contenido esencial del clausulado de estos modelos de acuerdo coincide sustancialmente: aceptación del EDI como medio de celebración entre las partes de acuerdos válidos; determinación, a menudo, del momento y lugar en que tales acuerdos se entenderán celebrados; admisibilidad como medio de prueba; medidas de seguridad, registro y almacenamiento de los mensajes de datos transmitidos a través de esta red cerrada; confidencialidad de los datos; requisitos técnicos para la explotación del EDI (equipos, programas de ordenador, medios de comunicación o estándares de transmisión y códigos de los mensajes); responsabilidad de las partes que suscriben el acuerdo y de quienes intervengan como intermediarios; cláusulas de sumisión judicial o arbitral; ley aplicable; efectos, y terminación del acuerdo[52].

Una de las principales ventajas de este tipo de acuerdos será la mayor confidencialidad y seguridad jurídica que imprime el hecho de poder pactar el régimen de las cuestiones que rodearan el intercambio de la información, a menudo carentes de regulación en los ordenamientos nacionales[53]. Para ello será necesario el compromiso, por los intervinientes, de dotar a los acuerdos alcanzados de la misma eficacia que los concluidos a través del intercambio de documentos en papel o en redes abiertas como Internet[54].

Así entendido, el EDI representa una actividad en red encaminada, fundamentalmente, a la realización de operaciones propias de comercio electrónico (SSI por excelencia), practicado inicialmente entre empresas (B2B). Es por esta razón que, con la aparición y avance de Internet y su generalización como marco de desenvolvimiento de las relaciones entre individuos con fines de todo tipo –especialmente comerciales– se acelera el decaimiento de los entornos cerrados, que tienden a ser sustituidos[55]. Ello no impedirá, sin embargo, un desa-

[51] DOCE L 338, de 28 de diciembre de 1994, p. 98.

[52] BOSS, A./RITTER, J. B., *Electronic Data Interchange agreements: a guide and sourcebook*, París, International chamber of commerce, 1993, pp. 41 a 113.

[53] CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, Madrid, Consejo General del Notariado, 2006, p. 27.

[54] HORNING, R. A., «The enforceability of contracts negotiated in cyberspace», *International journal of Law and information technology*, vol. 2, 1997, p. 119.

[55] SÁNCHEZ COLL, A., «Del EDI al comercio electrónico», *El comercio en la SI*, vol. 813, 2004, pp. 43 a 54.

rrollo paralelo de mercados electrónicos cerrados, en los que sólo participarán quienes pueden acceder a ellos tras haber aceptado contractualmente las condiciones que regulan su acceso y funcionamiento[56]. La regulación del funcionamiento de estos sistemas cerrados a través de sus acuerdos específicos resulta posible por la exclusión de los mismos del ámbito de aplicación de la legislación general en materia de identificación electrónica y servicios de confianza para las transacciones electrónicas contenida en el RIE-SCTE[57], cuyo artículo 2.2 dispone, literalmente, que esta normativa no resultará aplicable «[…] a la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes»[58].

2. Surgimiento de la red global: una revolución llamada Internet

Como adelantamos en líneas anteriores, la gran revolución tecnológica, determinante de los cambios experimentados por la sociedad de la información y por los servicios que en ella se ofrecen, se produce con el nacimiento de la red abierta internacional por excelencia: *Internet*, *la Red de redes*, el, ya considerado por muchos, sistema adaptativo complejo más grande y de más rápida evolución en la Historia de la Humanidad[59]. Sus orígenes[60] se encuentran en la

[56] Para un estudio más profundo de este tipo de mercados, *vid.* RODRÍGUEZ DE LAS HERAS BALLEL, T., *El régimen jurídico de los mercados electrónicos cerrados (e-Marketplaces)*, Madrid, Marcial Pons, 2006, pp. 31 a 117.

[57] DOUE L 257, de 28 de agosto de 2014, p. 73. Este Reglamento es también conocido por sus acrónimos en inglés eIDAS y eTS.

[58] No obstante, como señala ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», en GAMERO CASADO, E. (coord.) *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, Valencia, Tirant lo Blanch, 2017, p. 714, «[e]sta exclusión puede resultar inconveniente en el ámbito privado, dado que en este caso no se podrá acudir a las presunciones legales asociadas a los servicios de confianza».

[59] FORO DE DAVOS, *Consejo para la Agenda Global*, 2013, pp. 1 y ss.

[60] DI COCCO, C. Y OTROS, *Temi di Diritto dell'informatica*, cit., pp. 7 y 8; FIORELLI, G. I., *Il contratto elettronico tra armonizzazione materiale e Diritto internazionale privato*, Padua, Cedam, 2006, pp. 3 a 5; LEINER, B. M./CERF, V. G./CLARK, D. D. Y OTROS, «A brief history of the Internet», *Internet society*, vol. 5, 1997, pp. 22 a 31; MARTÍNEZ SÁNCHEZ, R./GARCÍA BELTRÁN, A., «Breve historia de la informática», *División de informática industrial*, vol. 1, 2000, pp. 1 a 20; MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., pp. 30 a 34; SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., pp. 201 a 213; SCOTTI, L. B., *Gobernanza global: alternativas para la regulación jurídica del ciberespacio*, Buenos Aires, Fedye, 2015, pp. 65 a 69.

aparición, en 1961, del primer documento sobre conmutación de paquetes, que propició la aparición, al año siguiente, del proyecto estadounidense ARPA, dirigido por Joseph Carl Robnett Licklider, y la creación, en 1969, de ARPANET, de la mano de Paul Varan, red experimental diseñada en investigaciones promovidas por el Departamento de Defensa de los Estados Unidos con el objetivo de establecer una red informática de comunicación que tuviera la capacidad de redirigir automáticamente la información (dividida en paquetes para poder asegurarla) por el camino adecuado para alcanzar su destino, evitando el colapso de partes de la red. En 1972 se crea el primer programa de correo electrónico (Ray Tomlinson), que se ve impulsado por la necesidad, manifestada por los desarrolladores de ARPANET, de un mecanismo sencillo de coordinación. Llegamos, así, a 1973, momento en el que surge la conexión de los primeros ordenadores fuera de Estados Unidos, propiciando el inicio de la *globalización digital*.

Ya en 1977, se comprueba la fiabilidad de los protocolos TCP/IP entre redes gubernamentales de Estados Unidos, acordando, en 1983, su uso para Internet, término que nace de la síntesis de la expresión *INTERconnected NETworks* y que aparece por primera vez un año antes para referirse al sistema de ordenadores conectados entre sí generando una red, la cual se conecta, a su vez, con otra infinidad de redes. En él, los ordenadores pueden comunicarse de manera recíproca gracias a la existencia de un lenguaje común (TCP) y son identificados por una dirección única (IP, con la forma xxx.xxx.xxx.xxx, donde cada *x* es un número[61]), dando lugar al precitado sistema TCP/IP. El funcionamiento de este protocolo indica que cualquier mensaje de datos deberá ser dividido en segmentos de una longitud determinada y que estos serán convenientemente numerados para permitir la posterior reconstrucción de dicho mensaje; realizada esta labor, el protocolo Internet se encarga de marcar cada paquete de información con el número IP del destinatario de los datos[62]. También emplean este sistema de protocolos las redes tipo *Intranet* o *Extranet*, que, al igual que el EDI, constituyen (en

[61] Como indica PEÑA LÓPEZ, I., «Fundamentos tecnológicos del Derecho de la sociedad de la información», cit., p. 73, la primera y más importante reflexión que cabe inferir de este hecho es que la participación en Internet no es anónima, dado que siempre es posible localizar el ordenador que ha hecho determinada conexión y determinadas acciones en la Red, si bien no es tan inmediato hallar a la persona que lo hizo: si se trata de un ordenador doméstico en un hogar con un solo habitante, la facilidad de identificar a la persona es mucho mayor que si se trata de un ordenador de un telecentro en una gran ciudad.

[62] CAMACHO CLAVIJO, S., *Partes intervinientes, formación y prueba del contrato electrónico*, Madrid, Reus, 2005, p. 56. Por lo demás, los principales datos con los que IP marca cada paquete son direcciones de Internet de origen y

mayor o menor medida, respectivamente), entornos cerrados, si bien, a diferencia de aquel, operan dentro de Internet: mientras que *Intranet* permanece cerrada a una determinada organización y el acceso es restringido a sus miembros, *Extranet* sólo permite la conexión entre dos o más organizaciones, no posibilitando el acceso al público en general.

En 1988 nace IRC, un programa que permite la conversación de dos o más personas en directo a través de Internet. Poco después comenzaron a surgir redes similares que permitieron la conexión a nivel mundial en ámbitos diversos, como el universitario, el investigador, el empresarial o el particular, que, progresivamente, fueron conectándose entre sí gracias a la cooperación y el libre intercambio de información, que supieron sobreponerse a la competencia y a la propiedad[63]. Todo ello hasta llegar a 1990, momento en el que surge la verdadera aplicación que revolucionaría el uso de Internet: la *www*, diseñada conjuntamente por Tim Berners-Lee y por Roger Cailliau en el CERN de Ginebra para ayudar a mantener una red de hipertexto informativa. Para poder acceder a la información en el contexto, Marc Andreessen pone en circulación, en 1993, el *Mosaic*, que se convierte en el primer navegador por la www que, comenzando a comercializarse en 1994, afianza el uso público de Internet a partir de 1995.

3. Rasgos definitorios del nuevo entorno digital

El giro producido ha permitido un acceso paulatino, de todas las personas y desde cualquier parte del mundo (con las salvedades ya anotadas al hablar de los inconvenientes derivados de la conocida *brecha digital*), a información producida por otras personas y en otros (o los mismos) lugares del planeta[64]. En esta (r)evolución, que tiene como resultado el surgimiento de la sociedad de la información, Internet desempeña un papel fundamental como

---

de destino, números de protocolo y un *checksum*, es decir, una rutina de chequeo que le permite conocer si se ha producido algún error en la transmisión (MERCADO IDOETA, C., *Banca en Internet: marketing y nuevas tecnologías*, Madrid, Dykinson, 1999, p. 154).

[63] CASTELLS OLIVÁN, M., *La galaxia Internet: reflexiones sobre Internet, empresa y sociedad*, Barcelona, Plaza & Janés, 2001, p. 23.

[64] MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., p. 26; SCOTTI, L. B., «Los escenarios del Derecho internacional privado actual: globalización, integración y multiculturalidad», en FERNÁNDEZ ARROYO, D./MORENO RODRÍGUEZ, J. A. (coords.) *Derecho internacional privado y Derecho de la integración. Libro homenaje a Roberto Ruíz Díaz Labrano*, Asunción, Cedep, 2013, pp. 12 a 14.

paradigma de la estrecha colaboración entre los modernos medios de comunicación y la tecnología informática[65].

El término *Internet* podría traducirse como *redes interconectadas* y viene a expresar el nacimiento de un conjunto de redes que constituyen el sistema, abierto y sin propietario, de comunicación por excelencia, en clara contraposición al concepto de red cerrada y con propietario, del que el EDI y la Intranet, como hemos visto, constituyen los principales paradigmas. De ello se desprende que las características definitorias esenciales del nuevo proceso transformador son la *internacionalidad* general de las operaciones, la *desmaterialización* o *intangibilidad* de la información, la *deslocalización* o *descentralización* de sus fuentes, la *interactividad* de los medios, el *automatismo* de su funcionamiento y la *atemporalidad* de los procesos de comunicación. Tales características hacen de Internet algo distinto de cualquier otro medio de comunicación que, hasta este momento, haya podido existir[66].

De este modo, Internet, como red global, representa un nuevo modelo de comunicación abierta que, merced a la necesaria combinación de infraestructuras de tecnología informática y de telecomunicaciones y gracias a la existencia de un lenguaje técnico basado en un conjunto de protocolos TCP/IP, supera toda distancia que pueda existir entre sus intervinientes. De este modo, configura, en toda su extensión, un nuevo mundo virtual que, amparado en el empleo de un conjunto de aplicaciones (*www*, correo electrónico, intercambio de ficheros, videoconferencia o *chat*), permite a cualquier individuo acceder a toda una variedad de servicios (fundamentalmente comerciales) y utilidades amparados por la nueva sociedad de la información. Este intercambio de datos y de información entre personas físicas por medio de Internet puede producirse mediante comunicaciones de persona a persona (como es el caso del correo electrónico) o de modo automático, a través de conexiones con sitios virtuales

---

[65] DE MIGUEL ASENSIO, P. A., *Caracterización y organización de Internet: perspectiva jurídica*, Cizur Menor, Aranzadi, 2015, p. 2.

[66] CALVO CARAVACA, A./CASRRASCOSA GONZÁLEZ, J., *Conflictos de leyes y conflictos de jurisdicción en Internet*, Madrid, Colex, 2001, pp. 13 y 14;

[66] DI COCCO, C. Y OTROS, *Temi di Diritto dell'informatica*, cit., pp. 7 y 8; FIORELLI, G. I., *Il contratto elettronico tra armonizzazione materiale e Diritto internazionale privato*, cit., p. 5; SCOTTI, L. B., *Contratos electrónicos: un estudio desde el Derecho internacional privado argentino*, Buenos Aires, Eudeba, 2012, pp. 34 a 36.

accesibles por cualquiera que utilice la Red (como sucede con el comercio electrónico propiamente dicho)[67].

Hay múltiples definiciones de Internet, que varían en función de la perspectiva predominante. Desde un punto de vista doctrinal, DE MIGUEL ASENSIO[68] define Internet como un entramado mundial de redes conectadas entre sí de un modo tal que posibilita la comunicación casi instantánea desde cualquier ordenador de una de esas redes a otros situados en otras redes del conjunto, concluyendo, como hemos podido anticipar, que se trata de un medio de comunicación global. También acierta FINOCCHIARO[69] cuando por Internet concibe una serie de conexiones descentralizadas y autosuficientes entre ordenadores y redes de ordenadores, capaces de transmitir rápida y, con frecuencia, automáticamente, comunicaciones sin una directa participación o control humano y con la posibilidad de desviar automáticamente las mismas sobre una ruta distinta si uno o más ordenadores son denegados o bloqueados; de este modo, Internet funciona como resultado de la participación de cientos de miles de operadores que deciden usar protocolos técnicos comunes para el intercambio de información conjunta.

Con anterioridad (24 de octubre de 1995) y desde una visión ciertamente más técnica, la FNC aceptó unánimemente una resolución en virtud de la cual se proporcionaba una definición del término como:

> «[…] sistema global de información que está relacionado lógicamente por un único espacio de direcciones global basado en el protocolo de Internet (IP) o en sus extensiones, es capaz de soportar comunicaciones usando el conjunto de protocolos TCP/IP o sus extensiones u otros protocolos compatibles con IP y emplea, provee o hace accesible, privada o públicamente, servicios de alto nivel en capas de comunicaciones y otras infraestructuras relacionadas».

Más inteligible y posterior, la Conferencia de la Haya de Derecho internacional privado alude a Internet como «red de redes de ordenadores, los cuales se encuentran interconectados entre sí por líneas de telecomunicaciones, permitiendo, de este modo, llevar a cabo una serie

---

[67] FINOCCHIARO, G. D./DELFINI, F., *Diritto dell'informatica*, Milanofiori Assago, Utet Giuridica, 2007, p. 26.

[68] DE MIGUEL ASENSIO, P. A., *Derecho privado de Internet*, Madrid, Civitas, 2001, p. 27.

[69] FINOCCHIARO, G. D. Y OTROS, *Diritto dell'informatica*, cit., p. 25.

de actividades»[70]. Por último, en nuestro país, la RAE define Internet como «red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación».

4. Evolución de la tecnología Web

Enlaces a ordenadores remotos, accesos a archivos igualmente distantes y uso del correo electrónico fueron las primeras aplicaciones de Internet, gracias a las cuales la Red se convirtió, para muchos, en un importante instrumento de trabajo, más que herramienta para la interacción y la comunicación. Era, sin embargo, necesario un paso ulterior que posibilitase la *red global*, omnicomprensiva y tendencialmente abierta a todos. Este avance se produce definitivamente con la creación de la *wwww* o *Web*, un nuevo modelo de sistema informático que cambia radicalmente la concepción de Internet y, con ello, de la sociedad de la información. Como conjunto de documentos unificados (la *www* no es un *software*), la Web se sirve de una serie de estándares que permiten su identificación, creación y consulta; entre ellos destacan tres, que son aquellos que han permitido su comienzo: la URL, que, como subconjunto de la URI, permite identificar los objetos de la Web, designando en modo único tales objetos y especificando cómo pueden ser automáticamente detectados y solicitados; la HTML, que es el lenguaje utilizado para elaborar documentos hipertextuales, y la HTTP, que es el protocolo que disciplina la interacción entre el ordenador *cliente*, que solicita la página web, y el ordenador *servidor*, que la suministra[71].

La Web, como cualquier otra rama de innovación tecnológica, no es estática, sino que evoluciona de forma paralela a como lo hacen los nuevos hallazgos informáticos. De este modo, podemos ver cómo, a lo largo de su evolución, la Web ha ido pasando por distintos estados de desarrollo y de participación. A continuación, analizamos las distintas versiones de la Web, desde la *Web 1.0* originaria a la futura (pero casi incipiente) *Web 4.0*.

[70] CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO, *Electronic commerce and international jurisdiction*, 2000, pp. 1 a 46.

[71] SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., pp. 225 y 226.

### 4.1. La Web 1.0

La *Web 1.0* (cuyo nombre no aparece sino cuando nace la *Web 2.0*[72]) surge con los inicios de Internet y es el primer estado de la tecnología que se aplicaba en todos los sitios Web. Este primer modelo se caracteriza por ser únicamente de lectura, permitiendo a sus usuarios navegar pero no editar el contenido ni adaptar en modo alguno la página. Este contenido se limita a albergar los documentos (textos o archivos multimedia, canciones o películas, entre otros) que el ordenador visualiza en el formato solicitado, amén de información inteligible sobre aspectos varios que quiera transmitir quien la elabora[73].

Así las cosas, la Web 1.0 se caracteriza, no por la ausencia de contenidos, información, interconexión o cierto grado de creación, sino por el carácter estático de dichos elementos, siendo el autor de los datos la principal fuente de información[74]. En concreto, se trata normalmente de sitios corporativos, de noticias o de información específica, cuyo acceso podía ser, a lo más, consultado, lo que se traducía en una prácticamente inexistente interactividad entre los sujetos implicados. El perfil del usuario tipo en la Web 1.0 es, en esencia, pasivo, consumidor de la información que se transmite en la Red, que se asemeja a una gran biblioteca a la que se puede acceder con facilidad. Por tanto, en la Web 1.0 se sigue el paradigma del libro tradicional, de modo que sólo unas pocas personas con los suficientes medios técnicos y económicos podrán publicar los textos que otros muchos leerán[75].

### 4.2. La Web 2.0

A partir de finales de los noventa, fruto de la crisis de las empresas *puntocom*, se evidencia la necesidad de reorientar el mercado y, con él, los servicios ofrecidos en Internet. No obstante, no es sino hasta el año 2004 cuando, de la mano de Tim O'Reilly, se empieza a hablar

---

[72] REVUELTA DOMÍNGUEZ, F. I./PÉREZ SÁNCHEZ, L., *Interactividad en los entornos de formación on-line*, Barcelona, Uoc, 2009, p. 55.

[73] GALLEGO PEREIRA, M. D./BUENO ÁVILA, S./LÓPEZ JIMÉNEZ, D., *La Web 2.0: una visión empresarial y jurídica*, Cizur Menor, Aranzadi, 2014, p. 37.

[74] Como indica GARCÍA ARETIO, L., *De la educación a distancia a la educación virtual*, Barcelona, Ariel, 2007, p. 3, se creaban contenidos, se almacenaban y se interconectaban entre sí, aunque, ciertamente, estaban condicionados a ciertos sectores, ámbitos y al papel desempeñado por los autores.

[75] REVUELTA DOMÍNGUEZ, F. I. Y OTROS, *Interactividad en los entornos de formación on-line*, cit., pp. 56 y 63.

de la *Web 2.0* para referirse a la creciente participación de los usuarios de la Web en la creación de su contenido y al desarrollo de las infraestructuras informáticas que permiten tal intervención[76] (**anexo I**).

Ahora, la Web se convierte en un texto reescribible donde todos pueden participar, siendo este el principal atractivo que presentan, tanto y más que los contenidos suministrados por la propia industria cultural[77]. Internet adquiere una nueva configuración y se convierte, no sólo en el medio mediante el cual acceder a la información (Web 1.0), sino también en el espacio en el que poder desarrollar toda una suerte de inteligencia colectiva[78], en la que todos están habilitados para comunicar, llevar a cabo actividades de distinta naturaleza, expresarse, construirse una imagen pública, interactuar con otros individuos, esforzarse en la creación y actualización de conocimiento, participar en la cultura y contribuir al debate social y político[79]. Todos participamos de manera constante en la emersión de una plataforma global para la elaboración y la colaboración, dando nueva forma a cada aspecto de la actividad desempeñada por el individuo. Así, mientras que la antigua Web contemplaba una visión pasiva en el tratamiento de la información, la nueva alude a conceptos como *comunidad*, *participación* y *colaboración conjunta* para describir el proceso de adquisición y creación de conocimiento[80]. Esto lleva a algunos autores a afirmar que la Web 2.0 ha traspasado las fronteras de la misma Red, ya que la evolución de las herramientas tecnológicas ha conformado un marco social en el que la vida cotidiana de las personas no se concibe si no está vinculada, directa o indirectamente, a la Web[81].

---

[76] O'REILLY, T., *What is Web 2.0?: design patterns and business Models for the next generation of software*, Sebastopol, O'Reilly Media, 2005, pp. 1 a 24.

[77] CORDÓN GARCÍA, J. A./ALONSO ARÉVALO, J./GÓMEZ DÍAZ, R. Y OTROS, *Las nuevas fuentes de información: información y búsqueda documental en el contexto de la Web 2.0*, Madrid, Pirámide, 2012, pp. 281 y 282.

[78] EBERSBACH, A./GLASER, M./HEIGL, R., *Social Web*, Constanza, Uvk Verlagsgesellschaft, 2008, p. 23.

[79] SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., p. 236.

[80] TAPSCOTT, D./WILLIAMS, A. D., *Wikinomics: how mass collaboration changes everything*, Londres, Atlantic Books, 2010, p. 268.

[81] GALLEGO PEREIRA, M. D. Y OTROS, *La Web 2.0: una visión empresarial y jurídica*, cit., p. 41.

### 4.3. Hacia las Webs 3.0 y 4.0

Como venimos reiterando, el desarrollo de la tecnología no es estático, sino que se encuentra en constante evolución. Lo mismo sucede con la Web, que, dada su estrecha vinculación con el mundo digital en el que se desenvuelve, no está ajena a esta a este proceso de transformación. Ello hace que, en la actualidad más reciente, se comiencen a emplear nuevos términos para dar respuesta a los cambios producidos tras la creación de la Web 2.0, habiendo quienes hablan ya de *Web 3.0* e, incluso, *Web 4.0*.

La primera de ellas se fundamenta en la conocida como *Web semántica*, entendida como Web extendida y dotada de mayor significado, en la que cualquier usuario podrá encontrar respuestas a sus preguntas de forma más rápida y sencilla, merced a la configuración de la información de una manera mejor definida. La Web 3.0 pretende construir una Web más inteligente, capaz de interpretar los términos utilizados en la búsqueda de información, mostrando, de este modo, los resultados más relevantes posibles al usuario[82]. Para ello, será preciso dotar a la Web de mayor significado (de ahí el término *semántica*) y contenidos, habiendo de estar sustentada por un lenguaje común que permita que la información sea totalmente accesible, permitiendo que los motores de búsqueda puedan interpretar los textos, de modo que, sobre la base de las preferencias de los usuarios, estas se combinen con los contenidos existentes en la Red, obteniéndose información más precisa y facilitando, en definitiva, la accesibilidad a los contenidos digitales[83]. Para la consecución de los fines expuestos, será necesario, como decimos, superar las dificultades planteadas por las diferencias interidiomáticas, perfeccionando los sistemas de traducción e interpretación existentes. También habrá de reducirse el protagonismo del sujeto en la búsqueda de información, incrementando las funciones de agentes inteligentes, cualificados para poder definir parámetros de búsqueda de forma autónoma[84].

La segunda, por su parte, también conocida como *Web ubicua*, supondría el siguiente paso en la evolución. Su eventual plasmación, que necesitaría de la creación de sistemas que sean

---

[82] *Ibid.*, p. 43.

[83] KÜSTER, I./HERNÁNDEZ, A., «From Web 2.0 to Web 3.0: antecedents and consequences of the attitude and use intention of social Networking in the semantic Web», *Universia Business Review*, vol. 37, 2013, pp. 104 a 119.

[84] PARRA VALCARCE, D., «De Internet 0 a Web 3.0: un reto epistemológico para la comunidad universitaria», *Anàlisi: quaderns de comunicaciò i cultura*, vol. 36, 2008, p. 68.

capaces de igualar la capacidad del razonamiento humano, tendría como objetivo principal el de vincular a personas con dispositivos, a fin de que, ambos, sean capaces de tomar decisiones conjunta y aunadamente[85].

## V. SOCIEDAD DE LA INFORMACIÓN Y DERECHO COMO FENÓMENOS YA INSEPARABLES

El advenimiento de la sociedad de la información comporta múltiples y sustanciales transformaciones sociales que, a su vez, generan nuevas exigencias, nuevos intereses y nuevos conflictos que requieren de disciplina jurídica. Vamos conformando paulatinamente un panorama general que, analizado si quiera mínima o someramente, plantea serios problemas ávidos de respuestas adecuadas y acordes a la seguridad que los sujetos de derechos y obligaciones, principales afectados por las incidencias de las nuevas tecnologías, necesitan para desenvolverse con suficiente confianza y de manera adecuada en un mundo virtual cada vez más inmerso en nuestra cotidianeidad. De esta manera, la regulación de la Red por el Derecho (o, lo que es lo mismo, la influencia del espacio digital en el ámbito jurídico, y viceversa) viene exigida por la peculiar naturaleza del medio técnico utilizado y requiere (se traduce) de (en) la adecuada combinación del Derecho *tradicional* con un Derecho *nuevo*, necesarios, ambos, en un contexto global que, caracterizado por la creciente diversidad y por la eclosión de importantes intereses comerciales, amenaza los valores de libertad, apertura y cooperación que caracterizaron los inicios de su proceso[86].

Como Derecho *tradicional*, el nuevo contexto planteará una problemática jurídica hasta el momento desconocida, propiciada, en esencia, por la desaparición del papel y de la firma manuscrita para el desenvolvimiento de relaciones negociales[87], cuestión que, de manera inexorable, desembocará en una revisión del viejo Derecho, es decir, del negocio jurídico, de las declaraciones de voluntad, del documento, de la autenticidad y la autenticación de la firma,

---

[85] GALLEGO PEREIRA, M. D. Y OTROS, *La Web 2.0: una visión empresarial y jurídica*, cit., pp. 44 y 45.

[86] DI COCCO, C. Y OTROS, *Temi di Diritto dell'informatica*, cit., p. 19.

[87] MARTÍNEZ NADAL, A., «La protección del consumidor en la Propuesta de Directiva sobre determinados aspectos del comercio electrónico», *Cuadernos de Derecho y comercio*, vol. 29, 1999, p. 114; MARTÍNEZ NADAL, A., «Comercio electrónico», en BOTANA GARCÍA, G. A./RUIZ MUÑOZ, M. (coords.) *Curso sobre protección jurídica de los consumidores*, Madrid, McGraw-Hill, 1999, pp. 247 y ss.; MADRID PARRA, A., «Contratación electrónica», en IGLESIAS PRADA, J. L. (coord.) *Estudios jurídicos en homenaje al profesor Aurelio Menéndez*, Madrid, Civitas, 1996, p. 2941.

de la prueba o de la seguridad jurídica en el tráfico (postura *instrumental*)[88]. Podemos afirmar, en consecuencia, que uno de los principales obstáculos que puede dificultar la expansión, primero, y consolidación, después, del modelo virtual se encuentra en la inadecuación de las vetustas fórmulas jurídicas para solucionar muchos de los problemas que conlleva el mundo digital, o, lo que es lo mismo, en la improcedencia de aplicar conceptos y categorías clásicas a transacciones comerciales que ya no lo son[89]. Esta circunstancia motiva la intervención del legislador para adoptar medidas legislativas que resulten adecuadas en orden a remediar, repetimos, muchas de las soluciones propuestas por el antiguo orden legal, adecuándolas a la realidad jurídica que ahora se nos plantea. El fin último que con esto se persigue no es otro que el de generar la confianza necesaria en los sujetos participantes para poder llevar a cabo operaciones jurídicas y económicas a través de estos modernos canales con una seguridad y eficiencia equiparables, en definitiva, a las existentes en el entorno físico[90]. Necesario será, por tanto, adaptar analógicamente (muchas veces por medio de la figura de la *remisión*) las viejas estructuras y los sectores jurídicos tradicionales (Derecho privado, Derecho administrativo, Derecho penal o Derecho procesal, entre otros) a los cambios introducidos por las modernas tecnologías de la información y de la comunicación. Todo ello sin modificar sustancialmente el Derecho original, rigiendo, en la medida de lo posible, el principio de inalterabilidad del Derecho preexistente[91].

Como Derecho *nuevo*, en muchos de los casos, dar respuesta a los cambios resulta imposible si estos no se ven acompañados de una paralela aparición e incorporación de sistemas y sectores hasta ahora desconocidos y, hasta cierto punto, inimaginables (postura *ontológica*).

---

[88] MIRANDA SERRANO, L. M. Y OTROS, *La contratación mercantil. Disposiciones generales. Protección de los consumidores*, cit., p. 337.

[89] OLIVENCIA RUIZ, M., «De nuevo la Lección 1.ª. Sobre el concepto de la asignatura. Discurso leído en la solemne apertura del curso académico», 1999, Universidad de Sevilla, pp. 1 a 65.

[90] CAVANILLAS MÚGICA, S., «Dieciocho recomendaciones para la empresa que practique comercio electrónico con consumidores», *Actualidad informática Aranzadi: revista de informática para juristas*, vol. 37, 2000, p. 1; GUERRERO CLAVIJO, R., «Novedades en materia de contratación mercantil introducidas por la Ley de Servicios de la Sociedad de la Información», *CEFLegal: revista práctica de derecho. Comentarios y casos prácticos*, vol. 47, 2004, p. 6; JIMÉNEZ DE PARGA CABRERA, R., «El comercio electrónico ¿seguridad jurídica?», *Derecho de los negocios*, vol. 118 y 119, 2000, pp. 3 a 12.

[91] ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., p. 333; VEGA VEGA, J. A., *Derecho mercantil electrónico*, Madrid, Reus, 2015, pp. 77 y 78.

Estos cambios no tienen que ver con la naturaleza de la relación, sino con la naturaleza técnica del medio empleado, en particular su carácter global, inmaterial y deslocalizado[92]. A veces, el medio técnico creará problemas jurídicos del todo nuevos, relativos a la existencia misma de la Red y a su modo de funcionamiento, mientras que, otras veces, atribuirá una connotación fáctica distinta a problemas jurídicos conocidos, como sucede con ciertos ilícitos que pueden ser más fácilmente cometidos en el medio virtual y cuyas consecuencias resultan amplificadas; en este último caso, la norma existe ya, pero será necesario proceder a adaptarla para poder hacer frente a los nuevos desafíos que se presentan[93].

Consecuencia de todo lo anterior, vemos que la conocida como *informática jurídica*, en cuanto disciplina unitaria, viene a bifurcarse en dos direcciones distintas: de una parte, la del *Derecho de la informática*, centrada en analizar y tratar de resolver los problemas jurídicos planteados por la informática (informática legislativa, judicial, administrativa y profesional) y en la que, por primera vez en la historia, el Derecho se hace dependiente de otra disciplina (la informática) para poder regular adecuadamente los acontecimientos sociales. De otra, la *informática del Derecho*, que estudia la utilización de la informática en el Derecho (en esencia, propiedad intelectual, protección de datos, documentos digitales, presencia virtual, comercio electrónico, gobierno electrónico, ciberdelincuencia o adecuación de la informática a los parámetros y exigencias constitucionales). Ambos, caras de una misma moneda, han conocido una enorme expansión en el curso de los últimos años, articulándose en sectores diversos que, en conjunto, han posibilitado de manera creciente el uso de las nuevas tecnologías como plasmación y realización de los derechos individuales y de las exigencias sociales[94].

---

[92] Tradicionalmente, como bien señala LORENZETTI, R., *Comercio electrónico: documento, firma digital, contratos, daños, defensa del consumidor*, Buenos Aires, Abeledo-Perrot, 2001, p. 37, ambas posturas han estado enfrentadas, surgiendo dos posiciones (las ya mencionadas postura *instrumental* –LEMLEY, M. A./LESSIG, L., *The end of end-to-end: preserving the architecture of the Internet in the broadband*, Los Ángeles, Ucla Law Review, 2000, p. 930; MUÑOZ MACHADO, S., *La regulación de la Red: poder y Derecho en Internet*, Taurus, Barcelona, 2000, p. 36; TROTTER HARDY, I., «The proper legal regime for 'cyberspace'», *University of Pittsburgh Law Review*, vol. 55, 1994, pp. 994 y 995– y postura *ontológica* –BOWREY, K., *Law & Internet cultures*, Cambridge, Cambridge University Press, 2005, p. 45; PASCUZZI, G., *Il Diritto dell'era digitale*, Bolonia, Il Mulino, 2006, pp. 22–) que, yo, entiendo compatibles.

[93] BARIATTI, S., «Internet: aspects rélatifs aux conflits de lois», *Rivista di Diritto internazionale privato e processuale*, vol. 550, 1997, p. 550.

[94] Para un estudio más pormenorizado de las relaciones entre Informática y Derecho a lo largo de estos años, *vid.* SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., pp. 16 a 41.

Es esta afirmación la que me lleva a la consideración, contrariamente a lo que pueda afirmar parte de la doctrina[95], de que estamos en presencia de un Derecho de carácter *horizontal* o *transversal* (si bien también especializado), que extiende y prolonga sus efectos sobre la práctica totalidad de ramas o vertientes jurídicas, precisamente como manifestación del efecto expansivo del que surge y al que acompaña: Internet. Además, la rapidez de los cambios exige una paralela celeridad (no siempre posible) de la producción normativa, imprimiendo unos ritmos cada vez más acelerados para poder estar actualizados[96]. Ello nos recuerda a lo que, ya en la primera mitad del siglo XX (1946), Carl Schmitt denominó *legislación motorizada*, describiendo el fenómeno caracterizado por la incontenible y frenética multiplicación y alteración que sufrían las leyes en los ordenamientos jurídicos contemporáneos, denuncia que fue reiterada con posterioridad (1953) por Ortega y Gasset[97].

Estamos, en definitiva, fruto del proceso globalizador que trae consigo la aparición de Internet como instrumento esencial del que se sirve la sociedad de la información, en presencia de un auténtico Derecho con vocación global, también conocido como *lex informatica*[98], propiciado, en gran parte, por su dimensión internacional y por la consiguiente desaparición

---

[95] Entre ellos, GARCÍA MEXÍA, P., «El Derecho de Internet», en PÉREZ BES, F. (coord.) *El Derecho de Internet*, Barcelona, Atelier, 2016, pp. 23 y 24.

[96] DI COCCO, C. Y OTROS, *Temi di Diritto dell'informatica*, cit., pp. 22 a 24.

[97] Ambos autores son mencionados, al hilo de esta cuestión, en la obra de GARCÍA DE ENTERRÍA MARTÍNEZ-CARANDE, E., *Justicia y seguridad jurídica en un mundo de leyes desbocadas*, Madrid, Civitas, 1999, p. 48.

[98] Las opiniones expresadas al respecto, inspiradas a menudo en conceptos de filosofía del Derecho, oscilan entre la concepción de Internet como *espacio sin ley* (*Cyberia*, como han dado algunos en llamarlo), por analogía con otros espacios ausentes de soberanía estatal (GIGANTE, A., «Blackhole in cyberspace: the legal void in the Internet», *The John Marshall journal of computer & information Law*, vol. 3, 1997, pp. 413 a 436), y la visión de Internet como fenómeno con un nuevo ordenamiento jurídico, a veces llamado *lex informatica* o *lex electronica*, propio de una *sociedad virtual* (BURNSTEIN, M. R., «Conflicts on the net: choice of Law in transactional cyberspace», *Vanderbilt journal of transactional Law*, vol. 29, 1996, pp. 75 a 90; DELACOURT, J. T., «The international impact of Internet regulation», *Harvard international law journal*, vol. 38, 1997, pp. 207 a 235; GAUTRAIS, V./LEFEBVRE, G./BENYEKHLEF, K., «Droit du commerce électronique et normes applicables: l'emergence de la lex electronica», *Revue de Droit des affaires internationales*, vol. 5, 1997, pp. 547 a 583; GOULD, M., «Rules in the virtual society», *International review of Law, computers & technology*, vol. 2, 1996, pp. 199 a 218; REIDENBERG, J. R., «Lex informatica: the formulation of information policy rules through technology», *Texas Law review*, vol. 3, 1998, pp. 553 a 593).

de las fronteras geográficas de cada una de las actividades que acaecen a su albergue[99]. Mientras que la revolución industrial podía ser regulada con relativa autonomía por parte de los distintos ordenamientos estatales (que, en esta época, se dotan de legislaciones internas mediante el fenómeno de la *codificación*), la repuesta jurídica a la informatización no puede ser circunscrita a nivel estatal, siendo necesaria la adopción de soluciones globales coordinadas y armonizadas que se adecuen de manera satisfactoria a la dimensión transnacional de las distintas actividades que las propician[100].

Todo ello determina, en definitiva, que la complejidad del fenómeno digital no pueda ser regulada en exclusiva por los Estados individualmente considerados, habiendo de acudir a mecanismos de coordinación y organización de carácter supranacional capaces de imprimir una respuesta suficientemente satisfactoria, equilibrada y uniforme a los problemas derivados del proceso expansivo que, de manera progresiva, se consolida[101]. Y todo ello con una, más que patente, dificultad añadida, cual es la naturaleza territorialmente delimitada de cada Derecho interno y soberano, difícilmente compatible con el carácter global propio de Internet[102]. En estos casos, la organización de intereses comunes en materias concretas se traduce en la determinación de normas a nivel supranacional que necesitan, no obstante, de normas de ejecución a nivel interno, es decir, de actos estatales de transformación de la norma internacional en norma interna (según la *teoría dualista*) o de adecuación del Derecho interno al Derecho internacional (según la *teoría monista*). De este modo, el monopolio normativo estatal viene erosionado[103], al menos en cuanto a la concreción del contenido de la norma, ya que el Estado se limita a dar, con el acto de ejecución, un *imprimatur* interno, obligatorio desde el

[99] Sentencia Tribunal Supremo norteamericano núm. 96/511, de 26 de junio de 1997, que declara la inconstitucionalidad de la Ley de decencia de las telecomunicaciones, del Congreso de los Estados Unidos. Para un estudio más profundo de esta sentencia, *vid.* FERNÁNDEZ ESTEBAN, M. L., «Limitaciones constitucionales e inconstitucionales a la libertad de expresión en Internet», *Revista española de Derecho constitucional*, vol. 53, 1998, pp. 283 a 311.

[100] SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, cit., p. 15.

[101] BARNES VÁZQUEZ, J., «La Internet y el Derecho: una nota acerca de la libertad de expresión e información en el espacio cibernético», *Cuadernos de Derecho judicial*, vol. 6, 1997, pp. 235 a 241.

[102] FINOCCHIARO, G. D. Y OTROS, *Diritto dell'informatica*, cit., pp. 3 a 42.

[103] MAESTRI, E., *Lex informatica: Diritto, persona e potere nell'età del cyberspazio*, Nápoles, Edizioni Scientifique Italiane, 2015, p. 95.

momento en que aceptan voluntariamente participar de la organización en cuestión[104]. Tal es el caso, a los efectos que aquí interesan, de las normas que forman parte del Derecho de la Unión Europea, que merman el domino estatal (exclusivo hasta la ratificación del Tratado de Roma y los sucesivos actos modificativos) sobre las reglas jurídicas aplicables a los particulares, hasta el punto de no necesitar, en muchos casos, de medidas internas de ejecución. Estas normas serán tomadas posteriormente como modelo de referencia por otras organizaciones regionales, ubicadas, fundamentalmente, en América del Sur y, en menor medida, en la zona del sudeste asiático[105]. A ello se une la incertidumbre a la hora de determinar, de una parte, los órganos competentes para resolver las cuestiones que se originan en este nuevo espacio y para garantizar la eficacia extraterritorial de las decisiones judiciales que se dicten al respecto y, de otra, la ley aplicable a los procesos que se originan en la Red[106].

## VI. SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN EN EL ORDENAMIENTO JURÍDICO ESPAÑOL: MARCO NORMATIVO REGULADOR

El verdadero reto de toda Ley que pretenda regular cualquier aspecto de la sociedad de la información será conseguir que ciudadanos y empresas incorporen la Red a su vida cotidiana. Para ello, el objetivo primordial de la norma tendrá que ser imprimir seguridad y confianza pero sin mermar, al mismo tiempo, la libertad de mercado[107]. Para la consecución de estos fines se crea, a nivel europeo, la DCE[108], que persigue contribuir al correcto funcionamiento del mercado interior, garantizando la libre circulación de los SSI entre los Estados miembros y aproximando determinadas disposiciones nacionales que resulten de aplicación, relativas a cuestiones tales como el establecimiento y responsabilidad de los PSSI, las comunicaciones

---

[104] FINOCCHIARO, G. D. Y OTROS, *Diritto dell'informatica*, cit., pp. 10 y 11.

[105] Sobre los aspectos concernientes al ámbito de extensión de los modelos comunitarios más allá de los confines geográficos europeos, *vid.* PANEBIANCO, M., *Introduzione al Diritto comunitario comparato: Diritto internazionale e Diritto dell'integrazione nell'Europa comunitaria e in America Latina*, Aix-en-Provence, Edisud, 1985, pp. 1 y ss.

[106] Sobre esta cuestión, resulta especialmente útil la obra, antes citada, de CALVO CARAVACA, A. Y OTROS, *Conflictos de leyes y conflictos de jurisdicción en Internet*, cit., pp. 13 a 167.

[107] CREMADES GARCÍA, J./GONZÁLEZ MONTES, J. L., *La nueva Ley de Internet: comentarios a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Las Rozas, La Ley-Actualidad, 2003, p. 80.

[108] DOCE L 178, de 17 de julio de 2000, p. 1.

comerciales, los contratos por vía electrónica, los códigos de conducta, los acuerdos extrajudiciales para la solución de litigios, los recursos judiciales y la cooperación entre Estados miembros[109]; además, completará el ordenamiento jurídico comunitario aplicable a los SSI, «[…] sin perjuicio del nivel de protección, en particular, de la salud pública y de los intereses del consumidor, fijados tanto en los instrumentos comunitarios como en las legislaciones nacionales que los desarrollan, en la medida en que no restrinjan la libertad de prestar servicios de la sociedad de la información» (artículo 1, apartados 1, 2 y 3, DCE).

Finalmente, de acuerdo con los apartados cuarto y quinto de dicho precepto, la presente Directiva, que no establece normas adicionales de Derecho internacional privado ni afecta a la jurisdicción de los tribunales de justicia[110], no será de aplicación en los siguientes casos[111]: en primer lugar, en materia de fiscalidad[112]; en segundo lugar, a cuestiones relacionadas con SSI incluidas en la DPPFTDP[113] y en la DTDP[114], que establecen ya un marco jurídico co-

[109] Es, esta, una Directiva de armonización (DÍAZ FRAILE, J. M., «El comercio electrónico: Directiva y Proyecto de Ley español de 2000. Crónica de su contenido, origen, propósitos y proceso de elaboración», cit., pp. 31 y 32).

[110] Sobre esta cuestión, *vid.* CALVO CARAVACA, A. Y OTROS, *Conflictos de leyes y conflictos de jurisdicción en Internet*, cit., p. 34.

[111] Como bien queda recogido en el considerando 12 DCE, esta exclusión viene motivada porque, en el momento de promulgación del texto, la libre circulación de SSI no podía quedar garantizada con arreglo al Tratado o al actual Derecho comunitario derivado; en otras palabras, se trata de contratos o actos jurídicos que contaban con una conexión tan fuerte e intensa con la soberanía estatal de cada Estado miembro que resultaba imposible justificar por razones de unidad de mercado interior o similares su transmisión legislativa a la UE, encontrándose, por ende, sustraídas de la regulación de la DCE.

[112] Con respecto a la letra a), el mismo considerando 12, *in fine*, hace mención expresa a esta concreta exclusión, al afirmar que las cuestiones fiscales y, más específicamente, el IVA (que, advierte, grava un gran número de SSI) deben quedar fuera del ámbito de aplicación de la DCE. Adicionalmente, el considerando siguiente deja bien claro que la DCE no busca establecer normas sobre obligaciones fiscales ni prejuzgar la elaboración de instrumentos comunitarios relativos a aspectos fiscales del comercio electrónico.

[113] DOCE L 281, de 23 de noviembre de 1995, p. 31. En la actualidad, esta referencia se ha de entender derogada en favor del nuevo RPPFTDP (DOUE L 119, de 4 de mayo de 2016, p. 1).

[114] DOCE L 24, de 30 de enero de 1998, p. 1.

munitario en materia de datos personales, razón por la cual no es necesario regular esta cuestión en la presente DCE[115]; en tercer lugar, a cuestiones relativas a acuerdos o prácticas que se rijan por la legislación sobre carteles; en cuarto lugar, a las actividades de los notarios o profesiones equivalentes, en la medida en que impliquen una conexión directa y específica con el ejercicio de la autoridad pública[116]; a la representación de un cliente y a la defensa de sus intereses ante los tribunales[117], y a las actividades de juegos de azar que impliquen apuestas de valor monetario, incluidas loterías y apuestas.

En España, es la LSSICE[118] la encargada de incorporar al ordenamiento jurídico interno la DCE[119]. Esta Ley tiene como objeto (artículo 1) la regulación del régimen jurídico de los SSI en lo atinente a las obligaciones y consiguiente régimen sancionador de los PSSI, las comunicaciones comerciales virtuales, la información (previa y posterior) que han de proporcionar, la validez y la eficacia de los contratos de naturaleza electrónica. Las disposiciones contenidas en esta norma, prosigue el precepto:

> «[…] se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado[120], o que tengan como finalidad la protección de la salud y

[115] Considerando 14 DCE. Para un estudio complementario de este aspecto, *vid.* GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, Oleiros, Netbiblo, 2009, p. 236.

[116] Así, el ejercicio de la autoridad pública, unido a la importancia de la fe pública, adquieren preeminencia respecto de la dimensión estrictamente comercial de tales actividades (*Ibid.*, p. 236).

[117] Aquí, por su parte, la conveniencia de velar expresamente por el derecho fundamental del ciudadano a la tutela de sus derechos e intereses ante los tribunales se considera prevalente respecto de la vertiente comercial de la abogacía (*Ibid.*, p. 236).

[118] BOE núm. 166, de 12 de julio de 2002.

[119] También, de modo parcial, la DAPIC (DOCE L 166, de 11 de junio de 1998, p. 51).

[120] El ámbito normativo coordinado, en términos expresados por la DCE –artículo 2.h) y considerando 21–, hace referencia a los requisitos exigibles a los PSSI en los regímenes jurídicos de los Estados miembros, independientemente de si estos requisitos son de tipo general o destinados específicamente a los mismos. Más concretamente, alude a las exigencias que el PSSI debe cumplir en relación con dos aspectos: de un lado, el inicio de la actividad de un SSI, donde se encuentran aquellas condiciones relacionadas con cualificaciones, autorizaciones o notificaciones; de otro, el ejercicio de la actividad de un SSI, como las exigencias relacionadas con el comportamiento del PSSI, con la calidad o el contenido del SSI (incluidos los aplicables a publicidad y contratos) o con la responsabilidad del PSSI. En cambio, el ámbito normativo coordinado no se refiere a aquellos requisitos aplicables a las mercancías en sí, a la entrega de las mismas o a los servicios no prestados por

seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia»[121].

De este modo, partiendo de la aplicación a las actividades realizadas por medios electrónicos de las normas tanto generales como especiales que las regulan, la LSSICE se ocupará tan sólo de aquellos aspectos que, ya sea por su novedad o por las peculiaridades que implica su ejercicio *online*, no se hallan cubiertos por dicha regulación (**anexo II**).

Por lo demás, siguiendo la línea marcada por el artículo 1.4 y 5 DCE, el artículo 5.1 LSSICE establece que, siendo SSI, se verán excluidos de su ámbito de aplicación tanto los prestados por notarios y registradores de la propiedad y mercantiles en el ejercicio de sus respectivas funciones públicas, como los prestados por abogados y procuradores en el ejercicio de las suyas de representación y defensa en juicio; todos ellos se regirán por su normativa específica. Las restantes materias contenidas en el artículo 1.5 DCE –apartados a), b) y c)– pero no en el artículo 5.1 LSSICE, correrán, en mi opinión, la misma suerte, dada la aplicación extensiva del Derecho comunitario. Por su parte, el apartado segundo del mismo precepto advierte que las disposiciones de la presente Ley, con la excepción de lo establecido

---

medios electrónicos. Este término es trasladado a nuestro ordenamiento jurídico interno, en términos prácticamente idénticos, en el anexo, apartado i), LSSICE, que delimita el ámbito normativo coordinado como el conjunto de requisitos exigidos aplicables a los PSSI, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, ya vengan impuestos por las leyes generales que les sean de aplicación; en todo caso, continúa, deberá referirse a los siguientes aspectos: en primer lugar, al comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas o los regímenes de notificación a cualquier órgano u organismo público o privado, y, en segundo lugar, al ejercicio posterior de dicha actividad, como los requisitos referentes a la actuación del PSSI; a la calidad, seguridad y contenido del SSI; a la publicidad y a la contratación electrónicas, o a la responsabilidad del PSSI. La LSSICE concluye advirtiendo que no quedan incluidas en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos.

[121] La LSSICE se completa con otras normas relativas a cuestiones varias, como contratación a distancia, protección de los consumidores, propiedad intelectual, pago electrónico, servicios financieros, protección de la intimidad y frente al tratamiento de datos o, a los efectos que aquí interesan, firma y sello electrónicos. Sobre esta cuestión, *vid.* PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», en PLAZA PENADÉS, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, p. 60.

en el artículo 7.1 LSSICE, serán aplicables a los SSI relativos a juegos de azar que impliquen apuestas de valor económico, sin perjuicio de cuanto se disponga en su legislación específica, ya sea estatal o autonómica; ello supone una aparente contradicción con lo dispuesto en el considerando 16 DCE, después plasmado en el tercer punto de su artículo 1.5.d), donde se establece expresamente la exclusión del ámbito de aplicación de la norma comunitaria de las actividades de juegos de azar que impliquen una participación con valor monetario, incluidas loterías y apuestas[122].

1. Concepto comprensivo de figuras heterogéneas

A nivel comunitario, fue manifiesto el interés que, desde un principio, suscitó el fenómeno de la sociedad de la información, tratando de evitar que las normas que los diversos Estados miembros dictaran en relación con los servicios prestados a su amparo pudieran suscitar divergencias susceptibles de perjudicar la realización del objetivo de integración económica y de libre prestación de servicios en el seno de la UE[123]. Como parece obvio, cualquier intervención legislativa en relación con estos nuevos servicios requería de una previa definición legal que permitiera, de un lado, delinear sus contornos esenciales, y, de otro, posibilitar su diferenciación respecto de otras prestaciones de distinta naturaleza. Se acuña, así, el término *servicios de la sociedad de la información*.

Al contrario de lo que pudiera pensarse, el texto normativo encargado de proporcionar una definición de SSI no es aquel que regula su objeto. En efecto, la DCE, en su artículo 2.a), efectúa una remisión al apartado segundo del artículo 1 DPINRT[124], modificada, a su vez,

[122] El objetivo que se perseguía con ello, concreta GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, cit., p. 236, era «[…] asegurar la protección de los consumidores –siempre vulnerables, pero aún más en el desarrollo de este tipo de actividades potencialmente adictivas hasta niveles patológicos– mediante normas específicas». No obstante, como advierte el considerando 16 DCE, esta exclusión no se refiere a los concursos o juegos promocionales en los que el objetivo sea fomentar la venta de bienes o servicios y en los que los pagos, de haberlos, sólo sirven para adquirir los bienes o servicios publicitados.

[123] PEGUERA POCH, M./TARRÉS VIVES, M., «Marco jurídico de los servicios de la sociedad de la información y del comercio electrónico», en PEGUERA POCH, M. (coord.) *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010, p. 319.

[124] DOCE L 204, de 21 de julio de 1998, p. 37.

por la DMDPINRT[125]; más tarde, esta definición será reiterada por el artículo 1.b) DPIMR-TRRSSI[126]. De acuerdo con este precepto, será SSI «todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios». Se entenderá que es *a distancia* aquel servicio que sea prestado sin que las partes se hallen presentes de manera simultánea, es decir, sin la presencia física sincrónica de la persona que presta el SSI (PSSI) y su destinatario (DSSI); *por vía electrónica*, cuando sea enviado desde la fuente y recibido por el DSSI mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe íntegramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético[127], y *a petición individual de un destinatario de servicios*, cuando sea este quien solicite que el servicio le sea prestado[128]. Por último, el SSI tendrá carácter *oneroso* cuando ambas partes intervinientes obtengan algo de manera recíproca, es decir, cuando tanto el PSSI como el DSSI realicen una prestación a favor de la otra parte[129]. Pese a esta última afirmación, conviene tener presente el contenido del considerando 18 DCE, que aclara que los SSI no cubren únicamente aquellos servicios que dan lugar a la contratación en línea, sino que, en la medida en que representen una actividad económica, serán extensivos igualmente a servicios que no son remunerados por sus destinatarios. En opinión de DÍAZ FRAILE[130], es esta naturaleza onerosa de la prestación una nota esencial, ya que lo que se incluye es toda actividad desarrollada por vía electrónica y que tenga un significado económico, más allá de que

[125] DOCE L 217, de 5 de agosto de 1998, p. 18.

[126] DOUE L 241, de 17 de septiembre de 2015, p. 1.

[127] Como señala PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., p. 46, lo que se quiere poner de manifiesto es que el SSI de que se trate debe prestarse a través de una red de comunicación, con independencia de cómo se produzca el acceso a la Red, ya sea por teléfono móvil, por televisión o por ordenador.

[128] *On demand*, de modo que los SSI están puestos a disposición de cualquier persona que lo desee, que podrá acceder a ellos de manera individualizada y en cualquier momento (*Ibid.*, p. 46).

[129] ARIAS POU, M., *Manual práctico de comercio electrónico*, Las Rozas, La Ley, 2006, p. 60.

[130] DÍAZ FRAILE, J. M., «El documento electrónico y la firma digital: su regulación en la Unión Europea», *Noticias de la Unión Europea*, vol. 177, 1999, pp. 17 y 18. En la misma línea, PLAZA PENADÉS, J., *Propiedad intelectual y sociedad de la información: Tratados OMPI, Directiva 2001/29/CE y responsabilidad civil en la Red*, Cizur Menor, Aranzadi, 2002, p. 229.

sea el usuario final, o no, el que deba pagar el servicio de que se trate. De este modo, se habrán de entender incluidos dentro de la noción de PSSI a todos aquellos que obtengan ingresos económicos como consecuencia del servicio, ya sea directamente (como es el caso de los servicios remunerados por sus destinatarios) o indirectamente (a través de la inclusión de publicidad o como consecuencia de la explotación de datos personales de los usuarios que se registran para acceder al servicio)[131]. Quedarían fuera, por contra, todos los demás supuestos en los que quepa apreciar una ausencia total de actividad económica, como suele ocurrir con las páginas o blogs de carácter personal, que deberán ser excluidos del régimen jurídico específico de los PSSI.

En concreto, del considerando 18 DCE se desprenden algunos SSI (enumeración, esta, no exhaustiva o *numerus apertus*) que se considerarán incluidos en el ámbito de aplicación de la norma. Entre ellos, cabría citar toda una amplia variedad de actividades económicas que se desarrollan en línea, en particular aquellas que consisten en la venta de mercancías por medios electrónicos. Ahora bien, como anticipábamos en líneas anteriores, dentro de esta noción se incluyen también, en la medida en que representan una actividad económica, servicios no remunerados por sus destinatarios, como los que consisten en ofrecer información en línea o comunicaciones comerciales; los SSIi que ofrecen instrumentos de búsqueda, acceso y recopilación de datos; los que cubren servicios consistentes en transmitir información a través de una red de comunicación, o los que permiten albergar información facilitada por el destinatario del servicio. Junto a los anteriores, también estarán comprendidos aquellos

[131] ADSUARA VARELA, B., «Algunas consideraciones previas sobre el comercio electrónico», *Información comercial española*, vol. 813, 2004, p. 16; DE MIGUEL ASENSIO, P. A., *Derecho privado de Internet*, cit., p. 134; LÓPEZ RICHART, J., «Difamación en la web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento», *Derecho privado y Constitución*, vol. 26, 2012, p. 160. Consciente de la dificultad que, en ocasiones, puede entrañar la determinación del carácter económico de un determinado servicio, PEGUERA POCH, M. Y OTROS, «Marco jurídico de los servicios de la sociedad de la información y del comercio electrónico», cit., pp. 320 y 321, compara seguidamente dos ejemplos claramente ejemplificativos al respecto y que constituyen extremos opuestos: un primer ejemplo, como sería el caso del buscador *Google*, donde el criterio de la obtención de ingresos indirectos por vía de publicidad es útil para apreciar la naturaleza económica de la prestación, y un segundo ejemplo, concretado en toda página web personal que se limita a incluir un simple *banner* publicitario, donde este mismo criterio no determina, *per se*, el carácter oneroso del servicio.

servicios que se transmitan entre dos puntos, como el vídeo a la carta o el envío por correo electrónico[132] de comunicaciones comerciales.

En cambio, prosigue el considerando anterior, no tendrán la consideración de SSI actividades como la entrega de mercancías en sí misma o la prestación de servicios fuera de línea, ni, tampoco, los servicios de radiodifusión televisiva[133] o radiofónica, ya que ninguno de ellos se presta a petición individual del destinatario de la prestación. El uso del correo electrónico o, por ejemplo, de sistemas equivalentes de comunicación entre individuos, por parte de personas físicas que actúan fuera de su profesión, negocio o actividad profesional, incluso cuando los usen para celebrar contratos entre sí, no constituirán, en ningún caso, un SSI[134];

---

[132] No encontramos en nuestro Derecho un concepto legal de *correo electrónico*. No obstante, el artículo 2.h) DPCE (DOCE L 201, de 31 de julio de 2002, p. 37), sí proporciona una definición al respecto. De acuerdo con la misma, se entenderá por correo electrónico «todo mensaje de texto, voz, sonido o imagen enviado a través de una red de comunicaciones pública que pueda almacenarse en la Red o en el equipo terminal del receptor hasta que éste acceda al mismo».

[133] Definidos en el artículo 1.e) DART (DOCE L 298, de 17 de octubre de 1989, p. 23), modificada, primero, por la DMDART (DOCE L 202, de 30 de julio de 1997, p. 60), y, después, por la DMDARTP (DOUE L 332, de 18 de diciembre de 2007, p. 27).

[134] Para entender este supuesto incluido en el ámbito de aplicación de la norma se requiere, por tanto, que el uso del correo electrónico (o de sistemas equivalentes de comunicación entre individuos) para realizar comunicaciones comerciales o, incluso, para celebrar contratos electrónicos entre sí, se realice por personas jurídicas o por personas físicas, siempre que, al menos una de ellas (el PSSI), actúe dentro de su actividad profesional. Resultado de lo anterior, cuatro situaciones se antojan posibles: en primer lugar, que el uso del correo electrónico (o de sistemas equivalentes de comunicación) se produzca entre personas jurídicas, es decir, que tanto el PSSI (que siempre ha de actuar en el marco de su profesión, negocio o actividad profesional) como el DSSI (que puede, o no, actuar en el marco de su profesión, negocio o actividad profesional) sean personas jurídicas; en segundo lugar, que el uso del correo electrónico (o de sistemas equivalentes de comunicación) se lleve a cabo entre una persona física y una persona jurídica, es decir, que el PSSI sea una persona física y el DSSI una persona jurídica o viceversa; en tercer lugar, que el uso del correo electrónico (o de sistemas equivalentes de comunicación) se realice por personas físicas, es decir, que tanto el PSSI como el DSSI sean personas físicas, y, en cuarto y último lugar, que el uso del correo electrónico (o de sistemas equivalentes de comunicación) se realice por personas físicas y que ninguna de ellas actúe en el marco de su profesión, negocio o actividad profesional, es decir, que ninguno de ellos tenga la consideración de PSSI (no teniendo el otro, por ende, la consideración de DSSI). Los tres primeros constituirán un SSI, no siendo así en el último de ellos. Para algunos autores (*Ibid.*, pp. 325 y 326), la mera comunicación efectuada por vía electrónica entre dos personas que actúan en un ámbito ajeno al de su profesión, negocio o actividad profesional, no significa que se estén prestando mutuamente SSI; es esta, entiende, la razón por la cual la DCE excluye expresamente este supuesto de la noción de SSI, dado

lo mismo sucederá con la relación contractual entre un empleado y su empresario o con aquellas actividades que, por su propia naturaleza, no puedan realizarse a distancia ni por medios electrónicos, entre las que se incluirían el control legal de la contabilidad de las empresas o el asesoramiento médico que implica el reconocimiento físico de un paciente.

Además, a la definición contenida en la DPINRT se acompaña una lista indicativa, contenida en su anexo V, en la que figuran expresamente servicios no cubiertos por este concepto. De acuerdo con la misma, no serán SSI aquellos que no sean ofrecidos a distancia, o, lo que es lo mismo, aquellos que se presten en presencia física del PSSI y del DSSI, aun cuando impliquen la utilización de dispositivos electrónicos (entre ellos se encuentran, entre otros, la revisión médica o tratamiento en la consulta de un médico con la utilización de equipo electrónico pero con la presencia física del paciente, la consulta en la tienda de un catálogo electrónico en presencia física del cliente, la reserva de billetes de avión a través de una red de ordenadores realizada en una agencia de viajes en presencia física del cliente o los juegos electrónicos en un salón recreativo en presencia física del usuario). Tampoco gozarán de esta consideración los servicios que no sean ofrecidos por vía electrónica, como son los que tienen un contenido material, aunque se presten utilizando dispositivos electrónicos[135] (habría que incluir aquí la expendeduría automática de billetes de banco o ferrocarril o el acceso a redes de carretera o aparcamiento de pago, aun cuando en las entradas o salidas haya dispositivos electrónicos que controlen el acceso o aseguren el pago adecuado); los que se prestan *off line* o fuera de línea (como la distribución de CD-ROM o de programas informáticos en disquetes), o los que no son prestados por medio de sistemas electrónicos de tratamiento o almacenamiento de datos (servicios de telefonía vocal, servicios de *fax* y *télex*, servicios prestados por medio de telefonía vocal o fax o consultas médica o jurídica o marketing directo por teléfono o fax). Por último, carecerán también de esta consideración los servicios

que no tendría sentido exigir en tal supuesto el cumplimiento de los requisitos que se imponen al PSSI. Yo tengo mis dudas al respecto, habida cuenta de que, desde un punto de vista estrictamente formal, el cumplimiento de los requisitos que forman parte del concepto de SSI sería causa justificativa suficiente para encuadrar también este supuesto dentro del ámbito de aplicación de la DCE, contribuyendo, así, a reforzar la certeza y seguridad jurídica de cuantos realizan una prestación por vía electrónica, máxime cuando tengan la condición de consumidores, ávidos de una especial protección jurídica que, de este modo, se vería ciertamente mermada.

[135] No hay que confundir este supuesto con el conocido como *comercio electrónico indirecto*, en el que, como tendremos ocasión de analizar más detalladamente, la ejecución de la obligación se efectúa por medios tradicionales, si bien el resto de fases se llevan a cabo de manera electrónica.

que no sean prestados a petición individual del destinatario mediante una comunicación individual (transmisión punto a punto), estando destinados, por tanto, a la recepción simultánea por un número ilimitado de destinatarios (transmisión punto a multipunto)[136]; se incluirían en este supuesto los servicios de *broadcasting* o radiodifusión, tanto televisiva (incluidos los servicios de cuasivídeo a la carta[137]) como sonora, y el teletexto (televisivo).

En nuestro ordenamiento jurídico interno, y en términos prácticamente idénticos, la LSSICE ha optado también por incluir, en el apartado a) de su anexo, una definición de SSI. Todos estos servicios, afirma el legislador español, se caracterizarán por cuatro aspectos esenciales que han de concurrir cumulativamente: ser prestados a distancia, por vía electrónica, previa petición individual del DSSI y, al menos habitualmente, a título oneroso. En concreto, con base en la Exposición de Motivos, el apartado tercero incluye dentro del concepto de SSI la contratación de bienes o servicios por vía electrónica[138], la organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales, la gestión de compras en la Red por grupos de personas, el envío de comunicaciones comerciales y el suministro de información por vía telemática[139]. Como podemos deducir de un análisis del texto, dentro de los SSI y, más concretamente, del comercio electrónico, se integrarían dos actividades fundamentales que agrupan al resto: de un lado, el envío de comunicaciones comerciales previas a la contratación, que agrupa el suministro de información vía telemática,

[136] Como acertadamente señalaran NESPOR, S./CESARIS, A. L., *Internet e la legge: la persona, la proprietà intellettuale, il commercio elettronico, gli aspetti penalistici*, Milán, Hoepli, 2001, p. 49, es esta una diferencia básica entre los servicios de telecomunicación y los servicios de radiotelevisión y radiodifusión, pues los primeros transmiten mensajes entre dos sujetos determinados, mientras que los segundos hacen lo propio entre un sujeto emitente y una pluralidad de sujetos receptores.

[137] Como vimos en el apartado anterior, el vídeo a la carta sí sería un SSI, a la vista de lo dispuesto por el considerando 18 DCE.

[138] El comercio electrónico y la contratación electrónica son dos realidades diferentes, toda vez que el primero, además de englobar a la segunda, comprende también otras actividades adicionales.

[139] El punto 18 de la D. D. LGCA (BOE núm. 79, de 1 de abril de 2010) eliminó el punto 6 de la letra a) del anexo LSSICE, que incluía entre los SSI, siempre que representase una actividad económica, «el vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la Red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual».

y, de otro, la contratación electrónica propiamente dicha, en la cual se subsume tanto la organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales como la gestión de compras en la Red por grupos de personas. Los medios a través de los cuales podrá canalizarse esta contratación serán, entre otros, el correo electrónico, la página web, la videoconferencia o el chat[140] (**anexo III**).

A ellos habrían de añadirse, como veremos, aquellos SSIi relativos a la provisión de acceso a la Red (*Internet service providers*), los que permiten la transmisión de datos por redes de telecomunicaciones (*mere conduit* o *routing*), los concernientes a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios (*proxy caching* o *memoria tampón*), los que posibilitan el alojamiento, en los propios servidores, de información, servicios o aplicaciones facilitados por otros (*hosting*), los que proveen instrumentos de búsqueda o de enlaces a otros sitios de Internet (*searching and linking*), los que hacen posible, tanto la creación, verificación y validación de firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, servicios de entrega electrónica certificada, certificados relativos a estos servicios y certificados para la autenticación de sitios web, como la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios (*trust services* –SSIisc–) o cualquier otro servicio que se preste a petición individual de los usuarios (como la descarga de archivos o audio), siempre que representen una actividad económica para el PSSIi[141] (**anexo IV**).

En cambio, no podrían reputarse como SSI aquellos otros que sean prestados por medio de telefonía vocal, fax o télex (no así la telefonía móvil cuando se accede a la Red[142]); el intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan[143];

[140] MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., p. 239.

[141] GONZÁLEZ GRANDA, P., «Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico», *Indret: revista para el análisis del Derecho*, vol. 4, 2007, p. 7.

[142] PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., p. 47.

[143] Así, como ya dijimos, el correo electrónico (u otro medio de comunicación electrónica equivalente) utilizado como medio exclusivo de comunicación entre particulares no será un SSI, sin perjuicio de que le sea de aplicación toda la normativa de protección de la intimidad en las telecomunicaciones (*Ibid.*, pp. 47 y 48).

los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta) contemplados en el artículo 3 de la LEART[144]; los servicios de radiodifusión sonora, y el teletexto televisivo y otros servicios equivalentes, como podrían ser las guías electrónicas de programas, ofrecidas a través de las plataformas televisivas.

2. Servicios de intermediación

Dentro de la noción de SSI, ocupa un lugar destacado aquella subcategoría que, como función general, permite que estos puedan ser prestados por el PSSI y utilizados por el DSSI. Hablamos de los SSIi, a los que tanto la normativa comunitaria como la nacional prestan una especial atención.

A nivel europeo, la DCE no contiene definición alguna de los SSIi, limitándose a emplear el término para identificar aquellos servicios para los que establece una exclusión de responsabilidad por los contenidos de terceros (artículos 12 a 15). Ha sido la LSSICE la que se ha encargado de establecer, por primera vez en nuestro ordenamiento jurídico interno, un concepto de SSIi. De acuerdo con la letra b) del anexo, será SSIi todo SSI por el que se facilite: a) la prestación o utilización de otros SSI o[145] b) el acceso a la información. De este modo, serán SSIi aquellos SSI instrumentales o accesorios cuyo objeto radique, precisamente, en facilitar la prestación (al PSSI) o utilización (al DSSI) de SSI o bien, simplemente, permitir (al PSSI o al DSSI) el acceso a determinada información[146].

Como hemos visto en el apartado anterior, entre los SSIi se incluyen: en primer lugar, los servicios relativos a la provisión de acceso a Internet (*Internet service providers*), cuyos prestadores se hallarán sujetos al régimen de responsabilidad contemplado en los artículos 12 DCE y

[144] BOE núm. 166, de 13 de julio de 1994. Esta norma ha sido derogada por la LGCA, cuyo artículo 2.2 define los servicios de comunicación audiovisual como aquellos cuya responsabilidad editorial corresponde a un prestador del servicio (persona física o jurídica que tiene el control efectivo, esto es, la dirección editorial, sobre la selección de los programas y contenidos y su organización en un canal o en un catálogo de programas) y cuya finalidad principal es proporcionar, a través de redes de comunicaciones electrónicas, programas y contenidos con objeto de informar, entretener o educar al público en general, así como emitir comunicaciones electrónicas.

[145] Entiendo que ambas funciones no son excluyentes, por lo que sería más conveniente haber introducido *y/o* en lugar de sólo *o*.

[146] PEGUERA POCH, M. Y OTROS, «Marco jurídico de los servicios de la sociedad de la información y del comercio electrónico», cit., p. 337.

14 LSSICE; en segundo lugar, los que posibilitan la transmisión de datos por redes de telecomunicaciones (*mere conduit* o *routing*), estando sometidos sus prestadores a cuanto disponen los preceptos anteriores; en tercer lugar, los servicios relativos a la realización de copia temporal de las páginas de Internet solicitadas por los usuarios o destinatarios (*proxy caching* o *memoria tampón*), cuya posible responsabilidad está recogida en los artículos 13 DCE y 15 LSSICE; en cuarto lugar se encuentran los servicios que permiten el alojamiento, en los propios servidores, de datos, aplicaciones o servicios suministrados por otros (*hosting*), donde los sujetos que se encarguen de su prestación se verán sometidos a lo establecido por los artículos 14 DCE y 16 LSSICE, en quinto lugar, aquellos que proveen instrumentos de búsqueda, acceso y recopilación de datos o enlaces a otros sitios de Internet (*searching and linking*)[147], contemplados legalmente por primera vez en el artículo 17 LSSICE[148], sin equivalente en la DCE[149] y, en último, lugar, los servicios de confianza que hacen posible, tanto la creación, verificación y validación de firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, servicios de entrega electrónica certificada, certificados relativos a estos servicios y certificados para la autenticación de sitios web, como la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios, agrupados en los artículos 3.16) y 17) y 13 a 45 RIE-SCTE.

3. Prestadores de servicios de la sociedad de la información

A su vez, conviene delinear el contorno legal de los sujetos encargados de la prestación de los SSI y SSIi anteriores. Para ello, deberemos acudir a dos cuerpos básicos: la DCE y, en un plano interno, la LSSICE, cuya conjunción, amén de, como veremos, el RIE-SCTE (este

[147] Como bien describe MONCADA FLÓREZ, J. P., *La responsabilidad de los prestadores de servicios de intermediación en la sociedad de la información*, Granada, Universidad de Granada, 2009, pp. 79 y 80, estos servicios se caracterizan por realizar rastreos de forma continuada e ininterrumpida en las webs existentes en la Red, a fin de identificar su contenido y proceder a su selección y clasificación sistemática, previa introducción en una base de datos electrónica para la puesta a disposición de sus destinatarios mediante el sistema de hiperenlaces, que conducen directamente al sitio mediante una simple pulsación sobre la dirección electrónica resaltada en el texto.

[148] El apartado segundo de este precepto se ha visto modificado por el artículo 4.7 LMISI (BOE núm. 312, de 29 de diciembre de 2007).

[149] Sobre estos SSIi, *vid.* CARBAJO CASCÓN, F., «Aspectos sustantivos del procedimiento administrativo para la salvaguarda de derechos de propiedad intelectual en Internet», *IDP: revista de Internet, Derecho y Política*, vol. 15, 2012, pp. 9 y 10; DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, Cizur Menor, Aranzadi, 2015, pp. 248 y 249.

último para los SSIisc) y la LFE[150]/ALSEC, será fundamental para obtener una visión adecuada de esta importante figura jurídica en toda su complejidad.

### 3.1. Concepto y caracteres

De acuerdo con el apartado b) del artículo 2 DCE, será PSSI cualquier persona, física o jurídica, que suministre un SSI[151]. A su vez, tendrá la consideración legal de *establecido* el PSSI «[…] que ejerce de manera efectiva una actividad económica a través de una instalación estable y por un período de tiempo indeterminado», teniendo en cuenta que la presencia y utilización de los medios técnicos y de las tecnologías empleadas para prestar el SSI no constituyen, en sí mismos, el establecimiento del prestador. En idénticos términos se pronunciará posteriormente la LSSICE en la letra c) del anexo.

De todo lo anterior se desprende una conclusión clara: quien suministra un SSI siempre habrá de hacerlo en el marco de su actividad profesional, negocio o profesión. Y ello a diferencia del DSSI, que, como veremos, podrá actuar en su doble condición de profesional y/o de consumidor. Por tanto, no podrá ser PSSI cualquier persona, física o jurídica, que proporcione información particular en la Red, ya que es necesario que esa información cumpla los presupuestos legales exigidos normativamente para los SSI[152].

### 3.2. Prestadores de servicios de intermediación

Si un PSSI es aquella persona, física o jurídica, que proporciona un SSI y un SSIi es aquel SSI por el que se facilita la prestación o utilización de otro SSI o el acceso a la información, por deducción, un PSSIi será aquella persona, física o jurídica, que proporciona un SSIi. Su labor consistirá, en definitiva, en servir de puente entre quienes editan y crean los contenidos y quienes acceden a los mismos, posibilitando que la información facilitada circule, se aloje

---

[150] BOE núm. 304, de 20 de diciembre de 2003.

[151] Equivaldrá, por tanto, a la figura del *iniciador*, contenida en los artículos 2.c) LMCE, si quien genera y envía el mensaje de datos lo hace para prestar un concreto SSI.

[152] Así, a modo de ejemplo, señala PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., p. 55, el particular o la asociación que, a través de una página web, dé cuenta de aspectos propios, sin repercusión económica alguna, no tendrá la consideración de PSSI; en cambio, sí tendrá la condición de DSSI (más concretamente, de DSSIi) el particular que, en las mismas condiciones, aloje su página web en un servidor ajeno (propiedad de un PSSIi).

o sea accesible en la Red[153]. De este modo, la principal diferencia entre un PSSI y un PSSIi residirá en la actitud que adopte en relación con los contenidos: mientras que el primero interviene de manera activa respecto de la información, el segundo mantendrá una posición pasiva, sin participar en su creación ni en la decisión de hacerla comprensible[154].

Estos SSIi, concreta el apartado segundo de la Exposición de Motivos de la LSSICE, serán ofrecidos por operadores de telecomunicaciones[155], proveedores de acceso a Internet, portales, motores de búsqueda o cualquier otro sujeto que disponga de un sitio en la Red a través

[153] PLAZA PENADÉS, J., «La responsabilidad civil en Internet: su regulación en el Derecho comunitario y su previsible incorporación al Derecho español», *La ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*, vol. 3, 2001, p. 2172. En la misma línea, BUSTO LAGO, J. M., «La responsabilidad civil de los prestadores de servicios de intermediación en la sociedad de la información», *Actualidad jurídica Aranzadi*, vol. 54, 2002, p. 3, al afirmar que en la transmisión y difusión de los contenidos en Internet no sólo interviene el proveedor del producto o servicio (PSSI), sino que también lo hacen otros sujetos, en distinto grado y en diversas formas, refiriéndonos a los mismos con carácter general con el término de intermediarios (PSSIi), o RODRÍGUEZ LÓPEZ, N., «La cadena de valor en Internet: análisis de su estructura y agentes participantes», *Revista de la contratación electrónica*, vol. 62, 2005, p. 71, quien define a los PSSIi como elementos computacionales que se hallan a lo largo de la ruta de transacciones que tienen lugar en la web.

[154] MONCADA FLÓREZ, J. P., *La responsabilidad de los prestadores de servicios de intermediación en la sociedad de la información*, *op. cit.*, p. 47.

[155] Esta figura fue definida por la DCMST (DOCE L 192, de 24 de julio de 1990, p. 10). Según su artículo primero, esta categoría estaría integrada por todas aquellas «entidades públicas o privadas –incluidas sus filiales sujetas a su control– a las que un Estado miembro conceda derechos especiales o exclusivos para el establecimiento de redes públicas de telecomunicaciones y, en su caso, para la prestación de servicios de telecomunicaciones». En nuestro país, es la LGT (BOE núm. 114, de 10 de mayo de 2014) la que, en la actualidad, proporciona una definición de esta figura; de acuerdo con la misma, contenida en el apartado 26 del anexo II, serán tales las personas, físicas o jurídicas, que explotan redes públicas de comunicaciones electrónicas o prestan servicios de comunicaciones electrónicas disponibles al público y que han notificado al Ministerio de Industria, Energía y Turismo –en la actualidad, y merced al artículo 10 RDRDM (BOE núm. 267, de 4 de noviembre de 2016), esta competencia se ha atribuido al Ministro de Energía, Turismo y Agenda Digital– el inicio de su actividad o están inscritas en el Registro de operadores. Las empresas de telecomunicaciones constituyen, en definitiva, el mercado integrado por los sujetos que controlan las características técnicas inherentes a Internet. Este mercado, inicialmente monopolístico, ha pasado a ser liberalizado en un corto plazo de tiempo, lo que ha provocado el surgimiento de alianzas internacionales entre estos operadores, a fin de potenciar su presencia en el mercado global de las telecomunicaciones, permitiendo, al mismo tiempo, repartir los sustanciales costes implícitos que conlleva mantener, adaptar y, en su caso, crear las infraestructuras técnicas y materiales que soportan el tráfico de Internet y del resto de servicios vinculados al mundo de las telecomunicaciones. De todo

del cual realice alguna de las actividades indicadas, incluido el comercio electrónico. De este modo, interpretando esta afirmación en sentido amplio, podemos llegar a la conclusión de que cualquiera que tenga un sitio web y ofrezca sus servicios profesionales a través de este medio estará sujeto y deberá adecuar su actividad de naturaleza electrónica al cumplimiento del contenido de la normativa de aplicación en materia de SSIi[156].

Por último, señalan CAVANILLAS MÚGICA y PAYERAS CAPELLÁ[157], los PSSIi podrán clasificarse en función de los SSIi que presten: así, podremos distinguir entre quienes prestan SSIi básicos (es decir, quienes proporcionan por separado alguno de los SSIi antes enumerados) y quienes prestan SSIi avanzados (aquellos que facilitan conjuntamente más de un SSIi). En cualquier caso, por lo que al Derecho interesa, las obligaciones y responsabilidades serán asumidas en función de la actividad que desempeñen en un momento dado, atendiendo a las normas que las impongan[158].

4. Destinatarios de servicios de la sociedad de la información

Al igual que hicimos en el punto anterior, adecuado será también delinear el perfil de la contraparte en esta relación simbiótica, personificada en quienes utilizan los SSI (incluidos los SSIi) prestados por los PSSI (incluidos los PSSIi): los conocidos como DSSI (incluidos los DSSIi).

---

ello se ocupa de manera profusa GARCÍA COSO, E., «La Unión Europea y los operadores de telecomunicaciones», en BOTANA GARCÍA, G. A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 113 y ss. Sobre la necesidad de conseguir una aplicación racional y eficaz de las normas de competencia en el sector de las telecomunicaciones, como medio para asegurar un nivel de competencia adecuado en el mercado transfronterizo de los SSI, *vid.*, entre otros, PEÑA MARTÍNEZ, M. Á./CABALLERO SANZ, F., «La política de competencia y el sector de las telecomunicaciones en la UE», *Información comercial española*, vol. 747, 1995, pp. 87 a 104; SOTO, J./PÉREZ, J./FEIJÓO, C., «Veinticinco años de la sociedad de la información en España: evolución tecnológica, globalización y políticas públicas», *Economía industrial*, vol. 349, 2003, pp. 63 a 82.

156 DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 249.

157 CAVANILLAS MÚGICA, S./PAYERAS CAPELLÁ, M. M., «Los servidores de acceso y alojamiento: descripción técnica y legal», en CAVANILLAS MÚGICA, S. (coord.) *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Granada, Comares, 2005, pp. 3 y 4.

158 APARICIO VAQUERO, J. P., «Los consumidores y sus relaciones con los proveedores de servicios de la sociedad de la información», *Revista de la contratación electrónica*, vol. 89, 2008, p. 42.

### 4.1. Concepto y caracteres. La figura del consumidor

El apartado d) del artículo 2 DCE define al DSSI como aquella persona, física o jurídica, que utiliza un SSI, «por motivos profesionales o de otro tipo y, especialmente, para buscar información o para hacerla accesible»[159]. En términos prácticamente idénticos se pronunciará el también apartado d) del anexo de la norma española[160].

De cuanto precede podemos extraer cuatro posibilidades que podrían darse en torno a la figura del DSSI: en primer lugar, que se trate de una persona física que, actuando en el marco de su actividad profesional, utilice un SSI; en segundo lugar, que se trate de una persona jurídica que, actuando de igual modo en el marco de su actividad profesional, utilice un SSI; en tercer lugar, que se trate de una persona física que, no actuando en el marco de su actividad profesional, utilice un SSI, y, en cuarto lugar, que se trate de una persona jurídica que, no actuando tampoco en el marco de su actividad profesional, utilice un SSI. Estos dos últimos escenarios participarán de la naturaleza propia del consumidor, sujeto que, en principio, vendrá representado por aquella persona física que utilice un SSI por motivos ajenos a su actividad negocial –artículo 2.e) DCE–.

En nuestro país, sin embargo, este concepto (y, con ello, el ámbito de aplicación subjetivo) se amplía con el apartado e) del anexo LSSICE, que se remite al concepto de consumidor como persona física o jurídica en su momento establecido en el artículo 1 de la ya derogada LGDCU[161]. Así es, de acuerdo con el apartado segundo de dicho artículo, son consumidores o usuarios[162]:

---

[159] Esta definición, aclara el considerando 20 de la Directiva, abarca todos los tipos de utilización de los SSI, tanto por personas que suministran información en redes abiertas tales como Internet, como las que buscan información en Internet por razones profesionales o privadas. Para una aproximación a la noción de consumidor en el ámbito de la contratación electrónica, *vid.* VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 131 a 138.

[160] En torno a la falta de idoneidad en el empleo de este término por parte del legislador nacional, *vid.* ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., p. 246.

[161] BOE núm. 176, de 24 de julio de 1984.

[162] Aquí sólo hemos de referirnos al consumidor, pues ni la DCE ni la LSSICE incluyen en ningún momento la figura del usuario. En este sentido, PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., p. 56, sostiene que hubiera sido acertado que ambas normas hubieran incluido

> «[…] las personas físicas o jurídicas que adquieren, utilizan o disfrutan como destinatarios finales, bienes muebles o inmuebles, productos, servicios, actividades o funciones, cualquiera que sea la naturaleza pública o privada, individual o colectiva de quienes los producen, facilitan, suministran o expiden».

Esta norma se verá derogada, con efectos desde el primero de diciembre del año 2007, por el TRLGDCU[163], actualmente en vigor, que, en la misma línea que la norma precedente, define al consumidor o usuario como sigue (artículo 3):

> «A efectos de esta norma y sin perjuicio de lo dispuesto expresamente en sus libros tercero y cuarto, son consumidores o usuarios las personas físicas que actúen con un propósito ajeno a su actividad comercial, empresarial, oficio o profesión. Son también consumidores a efectos de esta norma las personas jurídicas y las entidades sin personalidad jurídica que actúen sin ánimo de lucro en un ámbito ajeno a una actividad comercial o empresarial»[164].

Por lo demás, el uso de Internet para la comercialización de bienes y servicios al público ha posibilitado la generalización del acceso al comercio electrónico desde una vertiente puramente doméstica, personal. El desarrollo de las nuevas tecnologías favorece la celebración creciente de relaciones de consumo, al facilitar el contacto directo del consumidor con empresas situadas en cualquier punto del planeta, ya sea de manera unidireccional (comunicación comercial *online*) o bidireccional (contratación electrónica). En último extremo, en el mundo virtual llegamos, incluso, a una progresiva difuminación de las nociones de empresario y de consumidor, que facilita la celebración de acuerdos entre partes que no se conocen y que, tanto más, pueden permanecer en el anonimato o hacer uso de seudónimos; en consecuencia, el desarrollo de ciertos servicios asociados a la denominada *web 2.0* ha dificultado

también el concepto de usuario en cuanto DSSI que utiliza un SSI por motivos no profesionales, pues, entiende, encaja mejor con muchas de las actividades existentes en la Red.

[163] BOE núm. 287, de 30 de noviembre de 2007.

[164] Tal y como, acertadamente, subraya GARCÍA MEXÍA, P., «El Derecho de Internet», cit., p. 127, no contempla la normativa de referencia, ni europea ni nacional, la problemática de los contratos con doble finalidad, es decir, de aquellos contratos en los que la finalidad está relacionada sólo en parte con la actividad comercial de la persona, física o jurídica. Cuando se da esta situación, únicamente se entenderá que la persona en cuestión tiene la condición de consumidor cuando la finalidad relacionada con la actividad comercial sea tan limitada que no predomine en el contexto general del contrato. En esta línea se pronuncia el considerando 17 de la Directiva 2011/83/UE.

sobremanera la determinación de si alguien actúa con un propósito ajeno a su actividad profesional, haciendo nacer supuestos prácticos especialmente controvertidos[165].

Así las cosas, si bien los conceptos de DSSI y consumidor pueden confluir en una misma persona (especialmente en el comercio electrónico B2C), son estos conceptos diversos, de suerte que habrá ocasiones en que esa coincidencia no tenga lugar (véase, entre otros, aquellos supuestos de comercio electrónico B2B, donde el DSSI no es consumidor, o aquellos otros en los que el PSSI es, a su vez, DSSIi de otro PSSI, en concreto de un PSSIi). Ello determinará la aplicación de un régimen jurídico distinto para cada supuesto específico, siendo de aplicación la normativa de protección de consumidores y usuarios únicamente cuando una persona reúna, al mismo tiempo, la condición de DSSI y de consumidor[166]. El objetivo, en este último caso, es el de proporcionar al DSSI todo un elenco de normas específicas dirigidas a garantizar que su nivel de protección cuando realiza transacciones comerciales en modo electrónico con un PSSI[167] sea equivalente al existente en el mercado tradicional, requisito, este, imprescindible para poder generar la confianza necesaria en esta nueva modalidad virtual[168], siempre que no se incurra, parece obvio, en una sobrecarga normativa o sobrerregulación que haga perjudicar el desarrollo de este mercado, esta vez del lado del PSSI[169].

---

[165] Sobre las dificultades que reviste la determinación del régimen jurídico aplicable en estos casos, *vid.* DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 36 a 38.

[166] PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., pp. 56 y 57.

[167] Evidentemente, en el comercio electrónico entre empresarios (B2B) o entre consumidores (C2C), este conjunto de normas no sería de aplicación, dado que no existe la situación de indefensión que tratan de solventar.

[168] CENDOYA MÉNDEZ DE VIGO, J. M., «La protección de los consumidores», en DE ROS CEREZO, R. M./CENDOYA MÉNDEZ DE VIGO, J. M. (coords.) *Derecho de Internet: la contratación electrónica y firma digital*, Cizur Menor, Aranzadi, 2000, p. 123; GONZÁLEZ GRANDA, P., «Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico», cit., p. 4.

[169] Destacando el paulatino crecimiento de las obligaciones impuestas a quienes desarrollan actividades a través de Internet y como ello puede perjudicar el comercio electrónico y fomentar conductas tendentes a su incumplimiento, *vid.* HAINES, A., *Verbraucher schützende informationspflichten für websites: bedarfsgerechte angaben oder überregulierung?*, Münster, Universidad de Münster, 2008, pp. 287 y 288; NORDHAUSEN, A., «Information requirements in e-commerce Directive and the proposed Directive on unfair commercial practices», en

### 4.2. Destinatarios de servicios de intermediación

No conocemos definición alguna, normativa o doctrinal, de DSSIi. No obstante, si partimos del hecho de que un DSSI es aquella persona física o jurídica, que utiliza, sea o no por motivos profesionales, un SSI y un SSIi es aquel SSI por el que se facilita la prestación o utilización de otro SSI o el acceso a la información, por deducción, un DSSIi será aquella persona, física o jurídica, que utiliza, sea o no por motivos profesionales, un SSIi.

Teniendo como referencia los SSIi a que aluden la DCE y la LSSICE, así como el reciente RIE-SCTE, podemos enumerar cinco categorías de DSSIi. En efecto, de acuerdo con la legislación comunitaria y nacional actualmente vigente, serán DSSIi todas aquellas personas, físicas o jurídicas, que utilicen, sea o no por motivos profesionales, un SSIi consistente: en primer lugar, en transmitir por una red de telecomunicaciones datos por ellas facilitados o en facilitar el acceso a la misma (*ex*. artículos 12 DCE y 14 LSSICE); en segundo lugar, en solicitar datos previamente facilitados por otros DSSIi a un PSSIi que los transmite por una red de telecomunicaciones con la única facilidad de hacer más eficaz esta transmisión ulterior, siendo almacenados, para ello, de forma automática, provisional y temporal (*ex*. artículos 13 DCE y 15 LSSICE); en tercer lugar, en albergar datos proporcionados por dicho DSSIi (*ex*. artículos 14 DCE y 16 LSSICE); en cuarto lugar, en utilizar enlaces a otros contenidos ajenos al PSSIi o en acudir a los directorios o instrumentos de búsqueda incluidos por los PSSIi en sus propios contenidos (*ex*. artículo 17 LSSICE), o, en quinto y último lugar, en crear, verificar y validar, en favor del DSSIi, firmas electrónicas, sellos electrónicos, sellos de tiempo electrónicos, servicios de entrega electrónica certificada, certificados relativos a estos servicios y certificados para la autenticación de sitios web, así como aquellos otros consistentes en preservar firmas, sellos o certificados electrónicos relativos a estos servicios de confianza –*ex*. artículo 3.16) y 17) RIE-SCTE–.

De este modo, quien utilice un SSIi actuará simultáneamente con una doble condición jurídica: a) si quien hace uso del SSIi es un PSSI, actuará, al mismo tiempo, como tal respecto del DSSI (en lo atinente a la relación que origina la comunicación principal) y como DSSIi respecto del PSSIi (en lo atinente a la relación secundaria que sirve de soporte a la comunicación principal); b) en cambio, si quien hace empleo del SSIi es el DSSI, actuará, al mismo

---

JANSSEN, A. (coord.) *Information rights and obligations: a challenge for party autonomy and transactional fairness,* Londres, Ashgate, 2004, pp. 49 a 67.

tiempo, como tal respecto del PSSI (en lo atinente a la relación que origina la comunicación principal) y como DSSIi respecto del PSSIi (en lo atinente a la relación secundaria que sirve de soporte a la comunicación principal).

Por lo demás, hemos tenido ocasión de ver que: a) DSSIi será aquella persona, física o jurídica, que utiliza, sea o no por motivos profesionales, un SSIi, y b) consumidor será aquella persona, física o jurídica, que actúa con un propósito ajeno a su actividad profesional. De la conjunción de esta doble afirmación podemos extraer una tercera, cual es que la persona, física o jurídica, que utiliza, por motivos no profesionales, un SSIi tendrá la consideración de consumidor DSSIi. Como tal, las relaciones comerciales en que intervenga (y siempre que su contraparte no sea otro consumidor) se verán amparadas por las normas de protección del consumidor, que serán de aplicación conjunta con el resto de disposiciones propias del negocio electrónico celebrado. Este concreto consumidor DSSIi participará de todo cuanto se ha dicho en el apartado general relativo a los consumidores de SSI (consumidores como DSSI), si bien teniendo en cuenta que los SSIi que utiliza han de estar destinados a su esfera personal; de lo contrario, huelga decirlo, no estaríamos en presencia de un consumidor sino de un empresario o profesional.

## VII. EL COMERCIO ELECTRÓNICO COMO ESENCIAL SERVICIO DE LA SOCIEDAD DE LA INFORMACIÓN

Como podemos advertir de todo cuanto precede, el comercio electrónico no es sino un servicio más de la sociedad de la información. El legislador, tanto nacional como comunitario, no ha perseguido regular en exclusiva el fenómeno del comercio electrónico, sino que su verdadero objeto viene conformado por la noción integral de SSI[170]. No obstante, sí que ha pretendido dotarlo de una importancia extraordinaria que se refleja en el propio título de la DCE (*Directiva sobre comercio electrónico*) y de la LSSICE (*Ley de servicios de la sociedad de la información y de comercio electrónico*)[171].

[170] BOTANA GARCÍA, G. A., «Noción de comercio electrónico», en BOTANA GARCÍA, G. A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 40 y 41.

[171] GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, Valladolid, Lex Nova, 2002, p. 27.

Conviene precisar que la aparición del comercio electrónico (y, por extensión, de las comunicaciones comerciales y de la contratación electrónica como ramificaciones fundamentales) no supone, en términos absolutos, la creación de una nueva institución hasta el momento desconocida. No constituye innovación alguna en materia de comunicación entre ausentes, ni un tema que se incorpore al elenco de las distintas formas de contratación, ni siquiera supone la modificación de las tradicionales comunicaciones con fines publicitarios[172]. La novedad reside en el conducto a través del cual el comercio empieza a desarrollarse[173]. Surgen, a partir de este momento, múltiples y variados medios técnicos (EDI, EFT, Intranet, Extranet) que permiten su desenvolvimiento electrónico, si bien, como hemos visto, es la creación de Internet la gran innovación tecnológica que permite un cambio cualitativo y cuantitativo en la expansión de este fenómeno, al ser la primera red de comunicación de libre acceso que utiliza estándares abiertos, no privados.

## 1. Noción

En términos clásicos, la palabra *comercio* hace referencia al intercambio físico, entre comprador y vendedor, de bienes o servicios a cambio del pago de un precio[174]. Por su parte, el vocablo *electrónico* alude al medio a través del cual se procesan y transmiten datos digitales[175]. Así las cosas, desde una perspectiva general, podemos definir la fórmula resultante como el conjunto de datos que, transmitidos a través de los mecanismos que proporcionan las nuevas tecnologías de la información y de la comunicación, persiguen fines de carácter negocial, es

[172] MIRANDA SERRANO, L. M. Y OTROS, *La contratación mercantil. Disposiciones generales. Protección de los consumidores*, cit., p. 337.

[173] Así se pronuncia, ARIAS POU, M., *Manual práctico de comercio electrónico*, cit., p. 41, quien sostiene que el *e-commerce* (en su terminología anglosajona) no es sino una nueva forma de realizar el comercio tradicional, si bien utilizando los medios que las nuevas tecnologías de la información y de la comunicación ponen a nuestro alcance. Consecuencia de lo anterior, sostiene, a esta actividad le serán de aplicación todas las normas que regulan el comercio tradicional y, además, las específicas del medio en el que se desarrolla

[174] SEOANE BALADO, E., *La nueva era del comercio: el comercio electrónico. Las TIC al servicio de la gestión empresarial*, Vigo, Ideaspropias, 2005, p. 1.

[175] IBÁÑEZ MUÑOZ, J., *Poder y autoridad en las relaciones internacionales: el control del comercio electrónico en Internet*, Barcelona, Universitat Pompeu Fabra, 2004, p. 234.

decir, de compraventa de bienes o prestación de servicios, debiendo incluir aquí las negociaciones previas y otras actividades ulteriores relacionadas, aunque no sean estrictamente contractuales[176].

De este modo, con el empleo del término *comercio electrónico* no sólo se está haciendo referencia al hecho de efectuar una compra o una venta mediante el uso de las nuevas tecnologías de la información y de la comunicación, sino que también se incluyen actividades anteriores (publicidad de los productos o búsqueda de información) y posteriores (servicio postventa o reclamaciones) a las mismas[177].

No existe en nuestro cuerpo normativo actual definición alguna de comercio electrónico, ni en la DCE ni en la LSSICE[178]. En cualquier caso, nadie parece poner en duda que cuatro

[176] MARTÍNEZ NADAL, A., *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, Civitas, 2000, p. 29. Por su parte, VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., sostiene que «[…] lo que determina que estemos en presencia de este tipo de comercio es la utilización de la herramienta electrónica de modo que tenga o pueda tener alguna influencia en la consecución del fin negocial o en el resultado de la actividad de que se trate».

[177] RODRÍGUEZ COHARD, J. C./BERNAL JURADO, E., «Las regiones objetivo 1 españolas en la sociedad de la información: el comercio electrónico como elemento de desarrollo», *Revista de estudios regionales*, vol. 67, 2003, p. 110; RODRÍGUEZ LÓPEZ, N./VÁZQUEZ ABAD, J./MARTÍNEZ CARBALLO, M., «El comercio electrónico y la asimetría de la información: una aproximación desde los costes de transacción», *Revista galega de economía: Publicación Interdisciplinar da Facultade de Ciencias Económicas e Empresariais*, vol. 1, 2003, p. 2. En este punto, existe una clara confrontación entre un sector de la doctrina que sostiene que los SSI coinciden con los que el comercio electrónico comprende habitualmente, y, otro, que defiende que la noción de SSI engloba una variedad más amplia de actividades que el comercio electrónico. Entre los primeros se encuentran autores como ILLESCAS ORTIZ, R., «Entre Europa y la nada: a propósito del Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico de 29 de septiembre de 2000», *Revista de la contratación electrónica*, vol. 11, 2000, p. 3 o VATTIER FUENZALIDA, C., «Responsabilidad contractual y extracontractual en el comercio electrónico», *Anuario de Derecho civil*, vol. 1, 2002, p. 72. Entre los segundos, DÍAZ FRAILE, J. M., «Comentarios a la Directiva y al Proyecto de Ley español de comercio electrónico de 2000: contenido y proceso de elaboración», *Revista crítica de Derecho inmobiliario*, vol. 663, 2001, p. 85.

[178] Ha desaparecido en la Ley española la definición que de comercio electrónico se incluía en versiones anteriores, como en el Anteproyecto de 18 de enero de 2001, que, en su artículo 2.a), lo concebía como «toda forma de transacción o intercambio de información comercial basada en la transmisión de datos por redes de telecomunicaciones, como Internet». Pese a ello, no han sido pocos los autores que han perseguido captar en pocas líneas sus rasgos definitorios. Entre ellos se encuentra DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 190, que circunscribe el comercio electrónico a «toda aquella actividad que tenga por objeto realizar una

operación de comercio utilizando herramientas electrónicas, de forma tal que tenga o pueda tener alguna influencia en la consecución del fin comercial o en el resultado de la actividad que se está desarrollando»; DE LA RICA, E., *Marketing en Internet y e-business*, Madrid, Anaya, 2000, p. 107, quien afirma, desde una perspectiva más económica que jurídica, que comercio electrónico «será cualquier actividad de intercambio comercial cuyas transacciones básicas (órdenes de compra, pagos, órdenes de entrega) se realizan electrónicamente»; DE ROSELLÓ MORENO, R., *El comercio electrónico y la protección de los consumidores*, Barcelona, Cedecs, 2001, pp. 15 y 16, que afirma que «se incluyen aquí todas las actividades previas y posteriores a la venta, englobando por tanto, todas las fases del negocio empresarial. Éstas abarcan, la publicidad, la búsqueda de información sobre productos, proveedores, la atención del cliente antes y después de la venta, la distribución de los bienes y servicios adquiridos y los pagos electrónicos»; GÓMEZ GÓMEZ, A./PUENTE GARCÍA, F. J./MITRE ARANDA, M., «Importancia del comercio electrónico y su incidencia en la logística de aprovisionamientos», *Ingeniería industrial*, vol. 2, 2004, p. 1, para quienes el comercio electrónico se puede definir, en sentido amplio, como «cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet» ; KALAKOTA, R./WHINSTON, A. B., *Electronic commerce: A manager's guide*, Nueva York, Addison-Wesley, 1997, p. 68, que entienden que el comercio electrónico es algo más que hacer negocios electrónicamente, concibiéndolo como «un canal de distribución alternativo que permite a los oferentes de bienes y servicios cambiar e integrar todo el proceso, desde la fabricación hasta el servicio al cliente, lo cual influirá tanto en la organización interna como en las relaciones con los consumidores, pasando, incluso, por las relaciones entre empresas»; MARTÍNEZ NADAL, A., «Comercio electrónico», cit., p. 248, quien afirma que esta novedosa canalización virtual de las relaciones comerciales englobará «todo intercambio de datos efectuado por medios electrónicos», habiendo, en todo caso, de circunscribirse «a las transacciones comerciales electrónicas, es decir, de compraventa de bienes o prestación de servicios, así como las actividades y negociaciones previas y otras actividades ulteriores que estén relacionadas, aun cuando no sean estrictamente contractuales, desarrolladas a través de los mecanismos que proporcionan las nuevas tecnologías de la comunicación»; MONTERO ELENA, M., «Incidencias del comercio electrónico en el Derecho comunitario», *Anuario de Derecho europeo*, vol. 1, 2001, p. 134, en cambio, sintetiza el concepto como «toda operación comercial realizada a través de Internet, tecnologías de world wide web, télex, telegrama y cualquier otro sistema que conceptualmente sea posible integrar en el término»; PAZ LLOVERAS, E., *Cómo exportar, importar y hacer negocios a través de Internet*, Barcelona, Gestión, 2000, p. 11, que lo describe como «cualquier forma de transacción comercial o intercambio de información en la que se utilizan las nuevas tecnologías de la comunicación entre empresas, entre empresas y sus consumidores, o entre empresas y la Administración pública, así como los mecanismos de pago telemáticos, dinero digital, métodos de seguridad en el comercio *online* y operaciones bancarias cibernéticas»; SANTAMARÍA DÍAZ, F./ESCOBAR ESPINAR, M., «Estrategias empresariales ante el comercio electrónico», *Información comercial española*, vol. 813, 2004, p. 188, entienden que el comercio electrónico «se verá integrado por cualquier actividad realizada en la Red con ánimo comercial, siempre que pueda originar que se efectúe una transacción de esta naturaleza, ya sea en la web o fuera de ella, en el mismo instante o más tarde»; VICENT CHULIÁ, F., *Introducción al Derecho mercantil*, Valencia, Tirant lo Blanch, 2004, p. 772, ve en el comercio virtual un «conjunto de operaciones comerciales llevadas a cabo por medios electrónicos, es decir, todas aquellas transacciones electrónicas realizadas con fines publicitarios o contractuales entre empresas o entre empresas y particulares», o VÁZQUEZ GALLO, E./BERROCAL COLMENAREJO, J. J., *Comercio electrónico: material para el análisis*,

son las categorías de actividades comerciales que, vinculadas entre sí, conforman el ciclo comercial electrónico: publicidad y promoción del producto (que podrá ser un bien, un servicio o un producto digital susceptible de ser entregado y recibido mediante una transmisión electrónica); pedido o compraventa; entrega o recepción, y facturación o pago[179].

2. Posibles clasificaciones

Una vez realizada esta aproximación conceptual, podemos efectuar distintas clasificaciones del comercio electrónico, atendiendo, igualmente, a criterios diversos. En concreto, los factores que serán tenidos en cuenta se circunscriben a: a) las características de los bienes o servicios que se comercializan a través de la Red, b) los agentes que intervienen para permitir el funcionamiento del comercio electrónico, c) el grado de complejidad de las actividades desarrollas en este nuevo contexto, d) la tecnología utilizada para el desenvolvimiento de las relaciones entre los sujetos intervinientes, e) el ámbito geográfico en el que se desarrolla y f) el modelo de negocio que se persigue implementar por medios electrónicos (**anexo V**).

Por lo que respecta, en primer lugar, a las características de los bienes o servicios que se comercializan a través de la Red, podemos establecer una distinción entre *comercio electrónico directo* y *comercio electrónico indirecto*[180]. El comercio electrónico directo aglutina todas aquellas operaciones que tienen lugar sobre bienes intangibles (la compra de un libro electrónico o de un billete de avión a través de Internet, entre otros), de modo que todo el *íter* comercial se produce en el espacio virtual[181]. Es esta una modalidad de comercio electrónico que aprovecha las potencialidades que ofrece Internet y sus tecnologías asociadas para facilitar, no sólo que los bienes o servicios se contraten y suministren a través de la Red, sino también que el

Madrid, Centro de publicaciones del Ministerio de Fomento, 2000, p. 1, que añade a la definición anterior las operaciones comerciales que tienen lugar entre particulares o entre empresas o particulares con la Administración pública.

[179] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *Building Confidence: electronic commerce and development*, Ginebra, 2000, pp. 14 y 15.

[180] VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 106 y 107.

[181] HEREDIA CERVANTES, I., «Consumidor pasivo y comercio electrónico internacional a través de páginas web», *Revista jurídica Universidad Autónoma de Madrid*, vol. 5, 2001, p. 72; SORIANO ATIENZA, F. J., «Comercio electrónico y grandes superficies», en RAMOS HERRANZ, I./ILLESCAS ORTIZ, R. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, p. 373.

pago se efectúe dentro del propio entorno electrónico en el que las partes interactúan, permitiéndoles prescindir de los medios de distribución tradicionales y disminuyendo, por tanto, los costes asociados a las transacciones comerciales[182]. Su generalización dependerá, parece evidente, de la confianza que genere la seguridad de su funcionamiento, especialmente cuando se desconoce la identidad de una contraparte que, además, se halla geográficamente distante[183].

En cambio, el comercio electrónico indirecto comprende aquellas transacciones efectuadas sobre bienes materiales, tangibles (la compra de un libro físico a través de Internet podría ser un claro ejemplo de este tipo). Esto provoca que, al menos, una o varias de las operaciones vinculadas a la fase de contratación electrónica en que se desarrolla esta modalidad de comercio electrónico (fundamentalmente la entrega) se haya de efectuar por medios tradicionales, como el correo o la mensajería, y, por ende, fuera del mundo virtual, de modo que la ejecución de la obligación coincide con la que se produciría en el comercio físico[184]. Por sus características, este tipo de comercio electrónico puede ofrecer inicialmente mayor confianza a los consumidores y usuarios (al contar, entre otras, con la posibilidad de efectuar el pago contra reembolso, una vez se reciba el producto), si bien limitan enormemente las posibilidades que ofrece el sistema[185].

---

[182] MADRID PARRA, A., «Seguridad en el comercio electrónico», en ORDUÑA MORENO, F. J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, p. 144.

[183] HORTALL I VALLVÉ, J./ROCCATAGLIATA, F./VALENTE, P., *La fiscalidad del comercio electrónico*, Valencia, Ciss, 2000, p. 72.

[184] DREYZIN DE KLOR, A., «Derecho aplicable al comercio electrónico», *Seqüência: estudios jurídicos e políticos*, vol. 50, 2005, p. 283; ECHEBARRÍA SÁENZ, J. A., *El comercio electrónico*, Madrid, Edisofer, 2001, pp. 28 y 29. Hay autores como DEL PESO NAVARRO, E., *Servicios de la sociedad de la información: comercio electrónico y protección de datos*, Madrid, Díaz de Santos, 2003, p. 22, o FELIÚ ÁLVAREZ DE SOTOMAYOR, S., *La contratación internacional por vía electrónica con participación de consumidores: la elección entre la vía judicial y la vía extrajudicial en la resolución de conflictos*, Granada, Comares, 2006, p. 9, que consideran a este un comercio electrónico imperfecto, en el que todas las fases del procedimiento se realizan de manera electrónica, a excepción del pago y la entrega de la cosa, que responden al modelo tradicional.

[185] DOMÍNGUEZ LUELMO, A., «La contratación electrónica y la defensa del consumidor», en ECHEBARRÍA SÁENZ, J. A. (coord.) *El comercio electrónico*, Madrid, Edisofer, 2001, p. 71.

Como podemos advertir de todo lo anterior, de las dos modalidades fundamentales de comercio electrónico, como son las comunicaciones comerciales y la contratación electrónicas, sólo esta última puede responder, indistintamente, al modelo de comercio electrónico directo y de comercio electrónico indirecto, mientras que la primera no podrá desarrollarse si no es a través de la Red. Se produce, con ello, una identificación entre los términos *comercio electrónico indirecto* y *contratación electrónica indirecta*, pues todo comercio electrónico indirecto tiene lugar, a su vez, mediante un acuerdo de voluntades plasmado por vía electrónica.

Si atendemos, en segundo lugar, a los agentes que intervienen para posibilitar el funcionamiento del comercio electrónico, podemos hablar de *comercio electrónico entre empresas*, *entre consumidores*, *entre empresas y consumidores*, *entre empresas y Administraciones públicas* y *entre consumidores y Administraciones públicas*[186]. El comercio electrónico entre empresas, también conocido como comercio electrónico B2B, atiende a las operaciones comerciales realizadas, exclusivamente, entre empresas (comercio mayorista) y desarrollas dentro del *e-commerce*[187]. Se trata, en definitiva, de redes de comunicaciones dedicadas a la comercialización de productos industriales y a la transmisión de la documentación (órdenes de pedidos, especificaciones, cargos o pagos) necesaria para las transacciones entre empresas[188]. Siendo la modalidad que, tradicionalmente, ha generado un mayor número de transacciones, su exponente más significativo se encuentra en el sistema EDI, analizado en líneas anteriores[189].

---

[186] VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 104 a 106.

[187] BRIZ ESCRIBANO, J./LASO BALLESTEROS, I., *Internet y comercio electrónico: características, estrategias, desarrollo y aplicaciones*, Madrid, Mundi Prensa Libros, 2000, p. 73; ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., p. 330; MELIÁN ALZOLA, L., *La gestión de la calidad en el comercio electrónico desde la perspectiva del cliente*, Santa Cruz de Tenerife, Fundación Fyde-Caja Canarias, 2005, pp. 44 a 46; SOLÉ MORO, M. L., *Comercio electrónico: un mercado en expansión*, Madrid, Escuela superior de gestión comercial, 2000, pp. 51 y 52.

[188] SÁNCHEZ GONZÁLEZ, G., «El sector emprendedor de las TIC, el comercio electrónico y la colaboración con usuarios», *Economía industrial*, vol. 370, 2008, p. 88.

[189] APARICIO VAQUERO, J. P./MORO ALMARAZ, M. J./BATUECAS CALETRÍO, A., *Internet y comercio electrónico*, Salamanca, Universidad de Salamanca, 2002, p. 179; ESCOBAR ESPINAR, M., *El comercio electrónico: perspectiva presente y futura en España*, Madrid, Fundación Retevisión, 2000, p. 33; GÓMEZ VIEITES, Á. M./CEREJIDO SAMOS, I./VELOSO ESPIÑERA, M., *Economía digital y comercio electrónico*, Santiago de Compostela, Tórculo Edicións, 2002, pp. 83 y ss.

Por su parte, el comercio electrónico entre consumidores o C2C, persigue poner en contacto a oferentes y demandantes, ambos sujetos particulares[190], que proceden al intercambio de correos electrónicos, al uso de tecnologías P2P o al desarrollo de un sistema de subasta[191] (por ejemplo, *eBay*) con fines comerciales. Empresas y consumidores podrán también comerciar entre ellos en lo que se conoce como comercio electrónico B2C[192] o C2B, donde las relaciones comerciales producidas vía electrónica tienen como partes a un empresario[193] y a un consumidor final o viceversa, respectivamente (comercio minorista)[194].

Junto a los anteriores, podrán desarrollarse también actividades de comercio electrónico entre empresas y Administraciones públicas (B2A o A2B). El primero (B2A) se produce con la realización virtual de las actividades que, tradicionalmente, han tenido lugar entre las empresas y los distintos niveles de la Administración pública[195], ya que esta última puede actuar como cliente de las empresas al requerir, en su condición de macroorganización de servicios, de un continuo suministro de aprovisionamientos[196]. El segundo (A2B) englobaría todos

---

[190] RODRÍGUEZ ARDURA, I., *Marketing.com*, Madrid, Pirámide, 2000, p. 36.

[191] La subasta electrónica representa un modelo de transacción económica, caracterizado por una deslocalización temporal, espacial y de precios, que se configura como uno de los sistemas más eficientes de distribución de recursos. La deslocalización *temporal* es consecuencia de la ausencia de límites en lo que a la duración de la subasta se refiere; la deslocalización *espacial* responde a la ruptura de la barrea que del espacio físico de una sala de subasta produce el medio virtual, y, por último, la deslocalización *de precios* no es sino la flexibilidad que, en relación a los mismos, se produce en función de la oferta y de la demanda, primando frente a un modelo de precios fijo. Sobre esta cuestión, *vid.* HUIDOBRO MOYA, J. M., «El modelo de negocio de las subastas electrónicas (e-Auctions)», *Bit*, vol. 164, 2007, pp. 60 a 63; SOLÉ MORO, M. L., *Comercio electrónico: un mercado en expansión*, cit., p. 64.

[192] Como con acierto pone de manifiesto DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 36, la reciente evolución de Internet ha contribuido a erosionar la tradicional diferenciación entre comercio electrónico B2B y comercio electrónico B2C.

[193] Empresario que, a su vez, puede operar íntegramente en línea o combinar estas operaciones con otras llevadas a cabo en el mercado físico (PLANT, R., *Ecommerce. Formulación de una estrategia*, Madrid, Prentice Hall, 2001, p. 86). En estos casos, hace constar ARIAS POU, M., *Manual práctico de comercio electrónico*, cit., p. 44, el empresario actúa en condición de PSSI, mientras que el consumidor lo hace como DSSI.

[194] PAZ LLOVERAS, E., *Cómo exportar, importar y hacer negocios a través de Internet*, cit., p. 12.

[195] *Ibid.*, p. 13.

[196] MELIÁN ALZOLA, L., *La gestión de la calidad en el comercio electrónico desde la perspectiva del cliente*, cit., p. 48.

aquellos servicios que ofrece la Administración pública a las empresas de forma telemática (gestión electrónica de la recaudación de tributos o información en la página web de un Ayuntamiento sobre las empresas existentes en el término municipal, entre otros)[197] y que obedece al carácter regulador de las primeras y al papel que ejercen estas últimas como sujetos pasivos de derechos y obligaciones; así, tanto la Administración pública, a la hora de aportar información y entablar comunicación con las empresas, como estas, solicitando información y entablando comunicación con aquellas para cumplir con sus deberes legales y fiscales, justifican estos flujos de intercambio virtual[198]. De esta manera, en el comercio electrónico A2B, lo habitual será que a la Administración pública no le resulte de aplicación la LSSICE, dado que no suele reunir los requisitos necesarios para adquirir la condición de PSSI; no obstante, sí será de aplicación el contenido de la Ley cuando la actividad realizada por la Administración tenga carácter económico y salga, por tanto, de lo que es el cumplimiento de sus funciones públicas (por ejemplo, venta de paquetes turísticos por parte de una entidad pública dependiente del Ayuntamiento)[199].

El comercio electrónico entre consumidores y Administraciones públicas se identifica con sus respectivos acrónimos en inglés, C2A y A2C. El comercio electrónico C2A es la plasmación electrónica de aquellas relaciones que tienen lugar entre el consumidor (sujeto activo) y los distintos niveles de las Administraciones públicas (sujeto pasivo)[200]. En sentido contrario (A2C), y conscientes de las ventajas que proporcionan las nuevas tecnologías de la información y la comunicación, las Administraciones públicas han procedido a configurar de manera progresiva lo que se conoce como *e-administración*, con el objeto de reducir costes y propiciar una mayor proximidad al ciudadano (pago de impuestos vía electrónica, por ejemplo)[201]; al igual que en el comercio electrónico A2B, será el papel que adopte la Administración pública

[197] ALONSO CONDE, A. B., *Comercio electrónico: antecedentes, fundamentos y estado actual*, Madrid, Dykinson, 2004, p. 16.

[198] MELIÁN ALZOLA, L., *La gestión de la calidad en el comercio electrónico desde la perspectiva del cliente*, cit., p. 48.

[199] ARIAS POU, M., *Manual práctico de comercio electrónico*, cit., p. 45.

[200] MELIÁN ALZOLA, L., *La gestión de la calidad en el comercio electrónico desde la perspectiva del cliente*, cit., p. 48.

[201] GONZÁLEZ GRANDA, P., «Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico», cit., p. 3.

respecto del sujeto pasivo lo que determina la subsunción, o no, de la misma en el ámbito de aplicación de la LSSICE.

Si, en tercer lugar, tomamos en consideración el grado de complejidad de las actividades desarrollas en este nuevo contexto, podremos hablar de *actividades poco complejas*, entre las que cabría incluir la promoción de la empresa, el soporte pre y post venta o su presencia electrónica[202], y de *actividades complejas*, como podría ser la venta y distribución de productos y servicios en el ámbito interno y transfronterizo, los pagos electrónicos o los procesos compartidos[203].

En cuarto lugar, y en función de la tecnología utilizada para el desenvolvimiento de las relaciones entre los sujetos intervinientes, podemos separar el *comercio electrónico cerrado* del *comercio electrónico abierto*[204].

El primero se desarrolla en redes cerradas propiedad de los participantes (organizaciones y/o empresas) y se presta a determinados usuarios que, con carácter previo, han estipulado la realización de operaciones comerciales a través de una red en la que, antes, han sido habilitados (puede ser este el supuesto de comercio electrónico entre empresas a través del sistema EDI); de este modo, los contratos que, en su caso, se celebren, se perfeccionarán y ejecutarán en redes cerradas de cuyo acceso se encuentran excluidos aquellos sujetos que carecen de una habilitación contractual previa y específica[205].

El segundo, por el contrario, se desarrolla en redes abiertas como Internet, donde no existe la necesidad de acuerdos bilaterales previamente negociados y las partes no tienen por

[202] BOTANA GARCÍA, G. A., «Noción de comercio electrónico», cit., p. 61.

[203] Esta complejidad se reduce si las operaciones se entablan entre agentes conocidos o que están habituados a operar recíprocamente con regularidad (*Ibid.*, p. 62).

[204] VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 107 y 108.

[205] ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., p. 330.

qué mantener, obligatoriamente, relaciones estables, favoreciéndose el desarrollo de operaciones ocasionales o a corto plazo entre los intervinientes, sin la existencia de contratos previos[206].

En quinto lugar, dependiendo del ámbito geográfico en el que se desarrolle, estaremos ante un supuesto de *comercio electrónico interno*, que tiene lugar dentro de las fronteras de un Estado[207] o de *comercio electrónico internacional o transfronterizo*, en contraposición al anterior. En este último podremos hablar, a su vez, de comercio electrónico *intracomunitario* y *extracomunitario*, según se desarrolle en el interior o en el exterior del territorio de la Unión Europea, respectivamente[208].

En sexto y último lugar, atendiendo al modelo de negocio que se persigue implementar por medios electrónicos[209], diferenciaremos entre *comercio electrónico basado en ventas*, *en publicidad*, *en intermediación* y *en suscripción*. El comercio electrónico basado en ventas agrupa a todas aquellas empresas que venden productos o servicios a través de Internet (tiendas virtuales, tiendas clásicas con servicios *online*, tiendas de productos digitales y ventas por catálogo). El comercio electrónico basado en publicidad, que abarca los negocios conocidos habitualmente como *portales*, se basa en la difusión por empresas de contenidos en los que se integra publicidad mediante la inserción de *banners*, constituyendo estos su principal fuente de ingresos; constituyen variantes de esta modalidad los portales *horizontales o genéricos*, los portales *verticales o temáticos* y las *comunidades de contenidos*. Por su parte, el comercio electrónico basado en intermediación se halla conformado por todas las empresas cuya actividad principal reside en actuar como intermediarios entre compradores y vendedores en un entorno virtual (se integran aquí los agentes comerciales, los mercados verticales B2B, los distribuidores, los centros comerciales virtuales, los grupos de compras, las subastas *online* y las subastas inver-

---

[206] ARIAS POU, M., *Manual práctico de comercio electrónico*, cit., pp. 46 y 47; BOTANA GARCÍA, G. A., «Noción de comercio electrónico», cit., p. 62.

[207] ARIAS POU, M., *Manual práctico de comercio electrónico*, cit., p. 46.

[208] BOTANA GARCÍA, G. A., «Noción de comercio electrónico», cit., p. 62; ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., p. 330.

[209] Esta clasificación está basada en la realizada por RAPPA, M., «Business models on the Web», en AA.VV. (coord.) *Managing the digital Enterprise*, Carolina del Norte, North Carolina University, 2002, p. 3.

tidas); con ello, facilitan la comunicación y las transacciones entre todas las partes intervinientes en una operación de comercio electrónico, sea de la naturaleza que sea, siendo en las comisiones recibidas por el ejercicio de estas funciones donde los intermediarios encuentran su principal fuente de ingresos. Por último, el comercio electrónico basado en suscripción se caracteriza porque, en él, el usuario paga una cuota determinada por acceder a una serie de contenidos de carácter exclusivo; esta cuota puede ser fija, donde se permite el acceso a todos los contenidos del sitio web reservados para clientes suscritos, o variable, que dependerá de los contenidos solicitados.

3. Ventajas, riesgos e inconvenientes

Internet supone la aparición de importantes mejoras en el desenvolvimiento cotidiano de quienes actúan como prestadores y de quienes lo hacen como destinatarios de una actividad de comercio electrónico. Al tiempo, como sucede con todo fenómeno de tamañas características, inevitable será también que venga acompañado de significativos perjuicios. Lo relevante en estos será, por tanto, determinar si aquellas sobrepasan a estos, de modo que podamos afirmar, sin temor a equivocarnos, que la revolución que han supuesto las nuevas tecnologías de la información y de la comunicación es, en términos generales, provechosa; de lo contrario, difícilmente podríamos sustentar todo estudio que tratara de defender la bondad de los cambios introducidos por este nuevo modelo socioeconómico[210] (**anexo VI**).

[210] La clasificación que se sigue es de elaboración propia, si bien se ha basado en aportaciones de distintos autores, a saber: AMAR RODRÍGUEZ, V. M., «La interculturalidad tecnológica: inforricos e infopobres», cit., p. 367; CAMACHO CLAVIJO, S., *Partes intervinientes, formación y prueba del contrato electrónico*, cit., pp. 26 a 31; CIACCI, G., *La firma digitale*, Milán, Il Sole 24 Ore, 2000, p. 43; DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 33 y 34; DELFINI, F., *Il commercio elettronico*, Milán, Egea, 1999, p. 30; DÍAZ FRAILE, J. M., «El comercio electrónico: Directiva y Proyecto de Ley español de 2000. Crónica de su contenido, origen, propósitos y proceso de elaboración», cit., p. 43; DOWNES, L./CUI, C., *Estrategias digitales para dominar el mercado*, Barcelona, Granica, 1999, p. 66; DREYZIN DE KLOR, A., «Derecho aplicable al comercio electrónico», cit., pp. 275 y 276; FINOCCHIARO, G. D. Y OTROS, *Diritto dell'informatica*, cit., pp. 25 a 29; GÁMIR, A., «Los procesos de cambio en los servicios personales y el comercio: autoservicio, telecompra y teleservicio», *Boletín de la asociación de geógrafos españoles*, vol. 24, 1997, p. 13; GOMES SOARES, F. S., «La prueba en la contratación electrónica de consumo», *Riedpa: revista de estudios sobre Derecho procesal y arbitraje*, vol. 3, 2009, pp. 4 y 7; GONZÁLEZ SERRANO, L. Y OTROS, «Comercio electrónico y empresa: panorama actual y perspectivas futuras», cit., pp. 92, 93 y 104; JIMÉNEZ DE PARGA CABRERA, R., «El comercio electrónico ¿seguridad jurídica?», cit., pp. 1 y 2; LORENZETTI, R., *Comercio electrónico: documento, firma digital, contratos, daños, defensa del consumidor*, cit., p. 52.; MIRANDA SERRANO, L. M./PAGADOR LÓPEZ, J., «La formación y ejecución del contrato electrónico: aproximación a una realidad

Dentro de los aspectos positivos que conlleva la aparición del comercio electrónico en la sociedad contemporánea podemos destacar, en primer lugar, la consecución de una *mayor actualización y eficiencia del sistema*. El comercio electrónico propicia la reducción de los períodos de importación y de exportación de innovaciones y de transferencia tecnológica, lo que permite un reajuste constante de los distintos elementos indispensables para mantener niveles adecuados de producción, de comercialización, de distribución y de atención a las necesidades de los clientes. Asimismo, si bien es cierto que se crean nuevas figuras intermedias hasta ahora desconocidas, en términos generales podemos afirmar que en este nuevo panorama se acorta del proceso de producción por la eliminación de gran parte de los eslabones de la cadena (mayoristas y minoristas) existentes en el comercio tradicional; la razón estriba en el contacto directo que, gracias a la Red, tiene lugar entre los PSSI, o entre cualquiera de los intermediarios, con el DSSI, haciendo posible la simplificación de los trámites y de los costes necesarios para que el cliente pueda adquirir el producto o servicio deseado.

Asimismo, el nuevo contexto virtual en el que nos desenvolvemos propicia una *mayor igualdad de oportunidades* entre los sujetos intervinientes. Internet es un mundo donde, con frecuencia, interactúan personas cuya respectiva identidad es desconocida. Esto, entre otras muchas consideraciones, pone de manifiesto una especialmente: los menores costes que supone la venta de bienes y servicios por medios electrónicos permiten la posibilidad de que pequeñas entidades puedan competir con otras de mayor tamaño y poder. Así, si lo comparamos con el comercio tradicional, el comercio electrónico imprime un mayor equilibrio de oportunidades entre todos los agentes del mercado, al eliminarse gran parte de los obstáculos dirigidos a impedir la entrada de nuevos competidores y facilitar un mayor aprendizaje por imitación, favoreciendo, en ambos casos, una mayor eficiencia y competitividad. De este modo, pese a la permanencia de ciertos factores distintivos, nuevos o heredados (a nadie

negocial emergente», *Estudios de consumo*, vol. 85, 2008, p. 78; MOLINÍ FERNÁNDEZ, F., «Ventajas, inconvenientes e impactos territoriales del comercio electrónico», cit., pp. 131 a 144; ROSELLO, C., *Commercio elettronico: la governance di Internet tra Diritto statuale, autodisciplina, soft Law e lex mercatoria*, cit., pp. 3 y 4; SÁBADA CHALEZQUER, C., «Interactividad y comunidades virtuales en el entorno de la world wide web», cit., pp. 139 a 166; SANJURJO REBOLLO, B., *Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, protección de datos, negocios audiovisuales, e-commerce, consumidores, marketing*, cit., p. 34; SCOTTI, L. B., *Contratos electrónicos: un estudio desde el Derecho internacional privado argentino*, cit., pp. 34 a 36; SENNINGER, S. F., «The information economy», *Montana Business Quarterly*, vol. 1, 2001, p. 2; SHAW, M. Y OTROS, *Handbook on Electronic Commerce*, cit., pp. 19 a 21; STOLL, P. T. Y OTROS, *Electronic commerce and the Internet*, cit., p. 162; VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 82 a 86.

escapa que un mayor poder de marca influirá a la hora de establecer redes de distribución o de almacenaje más eficientes o escalas de producción más elevadas), las desigualdades se aminoran o difuminan en este nuevo contexto espacial.

Junto a lo anterior, el comercio a distancia hace posible también una *mayor agilidad en el desarrollo del conjunto de actividades llevadas a cabo por medios electrónicos*. Se reduce el tiempo y el coste empleado para transmitir y para recibir comunicaciones comerciales de todo tipo y/o para cumplimentar cada una de las fases que conforman el procedimiento de contratación electrónica, con el consiguiente efecto positivo para las partes implicadas.

De igual modo, dadas las características que rodean su origen y posterior desarrollo, el comercio electrónico está dotado de un *componente internacional o transfronterizo muy acusado*[211], lo que favorece el comercio internacional de bienes y servicios, ampliando de manera prácticamente gratuita y en términos inimaginables el abanico de posibles destinatarios, quienes, a su vez, se benefician de una apertura igualmente extraordinaria de la cantidad de bienes y servicios que pueden adquirir en el nuevo entorno digital. Se posibilita, por tanto, desde una misma ubicación y sin necesidad de establecimiento material, una venta abierta a todo el territorio, interno y externo[212], pudiendo, incluso, acceder a mercados antes aislados o difícilmente accesibles por inviabilidad económica o por falta de rentabilidad suficiente[213]. A todo ello habría que añadir el efecto positivo de aquellos casos en que, aun cuando no se celebren contratos por vía electrónica, la información y/o publicidad suministrada a través de la Red pueda ser útil para lograr clientes en el mercado presencial; para identificar nuevos suministradores o socios, capaces estos últimos, a su vez, de captar nuevos clientes o nuevos

---

[211] Y es que, como bien expresaran en su momento ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., pp. 330 y 331, «los medios electrónicos, y previamente los grandes tratados universales en materia comercial y financiera, han aportado al ejercicio empresarial una dimensión global hasta ahora inexistente y también determinado la subsiguiente desaparición de las fronteras estatales».

[212] SANJURJO REBOLLO, B., *Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, protección de datos, negocios audiovisuales, e-commerce, consumidores, marketing*, cit., p. 36.

[213] Cierto es, como se desprende de la obra de HAGEL, J./ARMSTRONG, A., *Net gain: expanding markets through virtual communities*, Brighton, Harvard Business School Press, 1997, p. 144, que esta superación de las fronteras territoriales supone, en ocasiones, una mayor dificultad a la hora de realizar búsquedas especializadas, ya que esta globalización en el acceso a información comercial fomenta, al mismo tiempo, el exceso de la misma.

canales de distribución; para aprovechar distintos puntos de venta que permitan desahogar el almacenamiento y para favorecer la distribución; para utilizar las distintas zonas horarias que hagan posible desarrollar proyectos conjuntos con la misma u otras empresas durante las veinticuatro horas del día, o, en fin, para impulsar nuevas formas de trabajo o relaciones laborales más flexibles, como el teletrabajo[214].

Al mismo tiempo, *poder comprar y vender productos o servicios integrados en el entorno virtual a cualquier hora del día* es otra de las ventajas fundamentales del comercio electrónico. Con ello, el PSSI consigue tener un escaparate permanente al que el DSSI puede entrar y comprar sin necesidad de presencia personal, tan sólo mediante el sistema informático necesario para tramitar las órdenes de compra a través de la web de manera adecuada y satisfactoria, acortando el ciclo de venta y reduciendo los costes asociados al mantenimiento de establecimientos de carácter físico. No todo queda ahí: además de la ausencia de límites territoriales y temporales, Internet presenta igualmente la ventaja potencial de poder sortear con mayor facilidad, rapidez y bajo coste las distintas barreras administrativas, fiscales y políticas que puedan presentarse[215].

El contexto digital favorece también la apertura de *nuevas oportunidades de negocio*, ya que, en esta incipiente realidad *online*, cada vez más presente, un porcentaje relativamente elevado de cuanto en ella se ofrece tendrá por fin dar respuesta al alumbramiento paralelo de nuevas necesidades originadas. El resto de bienes y servicios buscarán, por su parte, satisfacer de manera tanto más eficiente carencias comerciales tradicionales.

---

[214] Para ello, sostiene MOLINÍ FERNÁNDEZ, F., «Ventajas, inconvenientes e impactos territoriales del comercio electrónico», cit., pp. 139 y 140, se han de superar dos dificultades básicas: la primera reside en lograr que las páginas web se sitúen adecuadamente en los buscadores, llamen la atención y sean visitadas, a ser posible sin tener que recurrir a una costosa propaganda adicional; la segunda es que no se puede, o no es aconsejable, utilizar de manera indiscriminada las listas de correo electrónico disponibles en la Red para difundir masivamente información, mucho menos si esta tiene un fin comercial. Para alcanzar este objetivo de internacionalización adecuada, sostiene, sería conveniente ofrecer información periódica y actualizada sobre temas que resulten de gran interés para un elevado número de usuarios y, una vez detectado este, distribuirla a todos aquellos que la soliciten.

[215] La superación de estos obstáculos es especialmente adecuada respecto de los productos digitales que forman parte del comercio electrónico directo, ya que pueden distribuirse íntegramente a través de la Red sin necesidad de transporte físico.

Además, *el comercio electrónico mejora la información y la especialización e imagen de marca*. La nueva sociedad de la información en la que nos encontramos inmersos no sólo mejora la información de naturaleza comercial que se ofrece al cliente, también posibilita una mayor adecuación de los canales de comunicación entre los distintos miembros de la empresa, tanto mejor si se utiliza una Intranet, es decir, una red de uso exclusivo para los empleados. Internet permite una mayor capacidad de aprendizaje o *know-how*, ya que, de manera casi instantánea, es posible adquirir un conocimiento adecuado sobre prácticamente cualquier aspecto del saber, en general, y sobre los distintos elementos que conforman la cadena de valor de la empresa o las necesidades específicas de los individuos, en particular. Mejora, en definitiva, el acceso a la información necesaria para obtener un mayor grado de especialización, al facilitar, no sólo el acceso a información ya conocida, sino a una mayor variedad y diversidad de fuentes, siendo frecuente que muchos de esos contenidos puedan obtenerse de manera gratuita o a un precio generalmente inferior al existente en el mundo presencial. Además, con frecuencia, el intercambio de información fluye más rápida y libremente, lo que favorece la realización de estudios de mercado con los que poder incrementar la eficiencia del proyecto. Por último, con la posibilidad, favorecida por la gratuidad de la Red, de realizar encuestas de opinión a clientes o posibles clientes a través de la web y del correo electrónico, la empresa puede mejorar su imagen de manera notable; para ello, resulta conveniente que estas decisiones tengan lugar al tiempo que se produce la inmersión virtual de la compañía, ya que, si no es así, la inadecuada imagen de la marca puede perjudicar sobremanera su presencia en el mundo *online*, en detrimento de posibles clientes y accionistas.

No podemos olvidar tampoco la *reducción* que, en este espacio, se produce *de determinados costes*, entre ellos los de tiempo y de desplazamiento. Las nuevas tecnologías de la información y de la comunicación han supuesto, en términos generales, una disminución de costes de muy diversa naturaleza, ostensibles si los comparamos con aquellos que se exigen para la apertura y mantenimiento de negocios comerciales presenciales. Dados los menores costes de producción y/o comercialización que conlleva el negocio virtual (abaratamiento de los costes de personal, de publicidad, de apertura o de almacenamiento, entre otros), los precios, en general, de los bienes y servicios que se comercializan en Internet son generalmente más baratos que los ofertados en las tiendas presenciales. Además, el DSSI cuenta, en todo momento, con la posibilidad de conocer el precio final de los productos en cada uno de los lugares en que estos se comercializan, cuestión esta que supone un freno a la política, a veces seguida en el mundo *offline*, de mantener unos precios más elevados en unas zonas que en

otras. Adicionalmente cabría, incluso, la posibilidad de obtener mejores precios (quién sabe si también calidades) fruto de la lucha competitiva; es el caso, por ejemplo, de la subasta inversa, donde, a diferencia de la subasta ordinaria (en la que los posibles compradores pugnan por obtener el producto pagando más que el resto), los vendedores rivalizan o disputan por obtener negocio del comprador vendiendo más barato que sus adversarios. En todo caso, la estrategia seguida será muy variada y dependerá de cuestiones tales como el tamaño de la empresa, la posición que tiene y quiere en el mercado o la capacidad económica con que cuenta para poder invertir.

En la situación descrita, las *posibilidades efectivas de elección se incrementan*, favoreciendo una compra más eficiente y satisfactoria gracias a la comparación simultánea (de precios, condiciones y características) de las múltiples ofertas existentes en la Red. De hecho, han surgido nuevas empresas que tienen por objeto mostrar al interesado, en tiempo real, las mejores ofertas (agrupadas atendiendo a criterios como precio, distancia, valoración o popularidad) para cada una de las categorías de bienes o servicios solicitados.

Podemos conseguir, además, una *mayor personalización de los productos*. El producto que se adquiere en el comercio electrónico suele individualizarse con facilidad al cliente que lo adquiere. De este modo, resulta posible acompañar frases, colores, diseños o imágenes que les otorgan un valor adicional frente a los ofertados en el mundo presencial, más ligados a la producción genérica en masa.

También se generan *mayores descuentos*, derivados de la organización de los interesados. De este modo, ambas partes se benefician de la operación: los PSSI, porque garantizan un volumen mínimo de ventas, y los DSSI, porque pueden adquirir, mediante un sencillo procedimiento, el bien o servicio a un precio menor al que lo hubieran obtenido de haber actuado de manera individual, consiguiendo, en definitiva, un mayor poder negociador del que tendría cada uno de ellos por separado[216].

Internet ha fomentado igualmente, por ser inspiradora de su misma filosofía, la *participación en primera persona en la creación de la información* que circula a través de la Red, fruto, en gran

[216] Es el caso, como anticipábamos al inicio, de las *comunidades virtuales*, entendidas como agrupaciones de individuos, hasta cierto punto estables, que someten a debate una o más cuestiones de interés común para ejercer presión conjunta, a fin de alcanzar el objetivo, por todos sus miembros perseguido, de mejoras específicas en materia comercial.

parte, del ejercicio por el DSSI de su derecho a la libertad de expresión (recuérdese cuanto se ha expuesto respecto de las Web 2.0, 3.0 y 4.0). Aplicado al *e-commerce*, esto se traduce en una mayor intervención de los DSSI en los productos que circulan en el entorno virtual, dado que, repetimos, las empresas tendrán más en cuenta las preferencias de los individuos para lograr un nivel superior de satisfacción y/o personalización que garantice un crecimiento paulatino y progresivo de esta nueva realidad comercial *online*.

Pese a todo lo anterior, la implantación y generalización de la Red tropieza con algunas incertidumbres jurídicas que hacen preciso el establecimiento de un marco legal adecuado, capaz de generar la confianza necesaria para el empleo del medio virtual. Así, en materia de *autenticación del autor, privacidad de los datos y confidencialidad y veracidad de la información transmitida*, es imprescindible, si se pretende fomentar el impulso de las bondades del comercio electrónico y su uso cada vez más cotidiano, reforzar la seguridad técnica de los elementos que lo conforman. Será preciso garantizar que el autor de un determinado mensaje o declaración de voluntad no sea suplantado por ningún otro sujeto, haciendo que la información negocial recibida tenga carácter vinculante; de igual manera, se habrán de evitar los posibles riesgos derivados de que el emisor o el receptor del mensaje nieguen, respectivamente, haberlo emitido o haberlo recibido o de que el contenido del mensaje llegue a ser conocido por quien no está autorizado para ello. Para combatir, en la medida de lo posible, estos riesgos, se ha procurado incrementar la seguridad técnica, mejorando aspectos relacionados con la autoría, la integridad, el rehúse y la confidencialidad de la información.

A ello se añade el *peligro*, siempre latente, *de recibir productos erróneos o defectuosos*. La inmaterialidad inherente a estos procesos causa desconfianza en el cliente, que no puede verificar en el momento de efectuar la adquisición el estado y las características reales del bien o servicio contratado. Para solventar este problema surge, no obstante, el derecho de desistimiento negocial, que permite dejar sin efecto el contrato celebrado sin necesidad de justificar la decisión y sin penalización de ninguna clase.

Asimismo, existe una *desconfianza patente hacia el mercado digital*, menor, bien es cierto, a medida que transcurre el tiempo y se refuerza la seguridad jurídica del proceso. El recelo que, en algunos sectores de la población (especialmente en aquellos pertenecientes a generaciones anteriores al *boom* de las nuevas tecnologías de la información y de la comunicación), suscita todavía el comercio electrónico ha ralentizado, si quiera en los primeros compases, su crecimiento y posterior desarrollo. Esta desconfianza es debida, como pusimos de manifiesto al

inicio, a la incertidumbre existente acerca de las validez y eficacia de las transacciones efectuadas por vía electrónica; a la dificultad para poder determinar la ley y la jurisdicción aplicables en caso de litigio dada la naturaleza transfronteriza que, con frecuencia, presenta este tipo de comercio; al desarrollo de prácticas de comercialización no solicitadas o engañosas; al empleo generalizado de los contratos de adhesión; a la complejidad que supone el acceso en condiciones óptimas de seguridad a servicios en línea públicos y privados; a la imposición de cláusulas contractuales abusivas; a la posibilidad de tramitar un pedido por simple pulsación de teclas; a la dificultad frecuente de la prueba; a la determinación del lugar y el momento en que se entienden perfeccionados los contratos concluidos por este medio, o a la responsabilidad de los sujetos y agentes intervinientes.

Junto a ello, la falta de los medios económicos, técnicos, culturales y sociales necesarios para poder adaptar las infraestructuras a los nuevos avances, hace que *ciertos países en vías de desarrollo padezcan un cierto retraso o subdesarrollo*, variable en función del territorio, respecto de aquellos países tecnológicamente más evolucionados. Esto origina, como hicimos constar, una clara separación entre *inforricos*, con óptimas posibilidades de conexión y acceso a la Red, e *infopobres*, en clara situación de desventaja respecto de los anteriores.

Además, aun cuando el empleo del comercio electrónico conlleva una reducción general de *costes*, es cierto que su implantación también hace nacer otros *hasta ahora inexistentes o significativamente menores*. Nos estamos refiriendo, fundamentalmente, a aquellos derivados de la apertura de una potente red de distribución capaz de asegurar la puesta a disposición del producto en cualquier parte del mundo y a un precio relativamente reducido para el cliente. Bien es cierto que algunas empresas (entre otras, *Amazon*) han optado por amortizar, en parte, este gasto, proporcionando a los clientes la posibilidad de disfrutar (a cambio de un coste adicional) de ciertas ventajas y de obtener un servicio de entrega más completo o rápido. Amén del anterior, son también de destacar aquellos otros costes de constitución e implantación requeridos por el nuevo sistema informático (no se trata, tan sólo, de contar con una página web informativa, sino que se exige una nueva estructura organizativa y un nuevo marco de análisis), de contratación de personal especializado en el sector o de publicidad.

Suele decirse también que quien actúa en la Red como DSSI lo hace, hasta cierto punto, *a ciegas*, ya que su decisión en torno a un concreto producto o servicio sólo ha podido basarse en la información suministrada por la contraparte, quien, como parece evidente, tratará de

hacer que su oferta sea lo más atractiva e interesante posible. Este contexto es especialmente peligroso en aquellos casos en los que el cliente es un consumidor, particularmente indefenso ante el doble peligro de desinformación e insuficiente formación.

Es frecuente afirmar igualmente que *el nuevo contexto electrónico*, en el que las ofertas son recibidas y aceptadas fuera de los lugares en los que tradicionalmente se celebran los contratos, *puede favorecer la irreflexión del DSSI*. A mi entender, esta situación de indefensión, efectivamente característica de otras modalidades de comercio a distancia, no responde a la naturaleza propia de la contratación electrónica, donde el destinatario de la oferta cuenta con la posibilidad de reflexionar adecuadamente sobre la adquisición en un ambiente tan propicio para ello como puede ser el de su propio domicilio, separado del PSSI y, a menudo, sin plazo específico para responder. No obstante lo anterior, a nadie escapa la existencia de múltiples técnicas, como el diseño de ciertas páginas web, que favorecen la adopción de declaraciones negociales impulsivas que habrá que ponderar.

A pesar de todo ello, como acertadamente afirmara MOLINÍ FERNÁNDEZ[217]:

> «[…] las ventajas empresariales de apostar por Internet no sólo parece que superan a los inconvenientes, sino que, desde hace algún tiempo, en la mayoría de los casos el no estar conectado a la Red representa una cierta desventaja comparativa, que será más o menos grave según el tipo de actividad. Sin embargo, para generar oportunidades vinculadas al fuerte crecimiento y al gran efecto multiplicador de las autopistas de la información, no basta con conectarse a Internet. Para obtener el mayor rendimiento posible, dicha conexión debe formar parte de una estrategia proactiva, es decir, tendente a generar oportunidades y a anticiparse a la competencia buscando ser los primeros en una curva de crecimiento rápido».

[217] *Ibid.*, p. 136.

# CAPÍTULO SEGUNDO

# VALIDEZ Y EFICACIA DE LOS CONTRATOS PRIVADOS CELEBRADOS POR VÍA ELECTRÓNICA

**SUMARIO**. - **I.** NATURALEZA DEL FENÓMENO CONTRACTUAL ELECTRÓNICO DESDE UNA PERSPECTIVA DOCUMENTAL: UN LASTRE HEREDADO. **1.** Teoría dualista tradicional: mismos problemas, distinto enfoque. **2.** Nueva propuesta: la teoría del documento como fin y el principio de equivalencia funcional como instrumento reparador. **3.** Elementos esenciales y clasificación actual del documento. **II.** COMUNICACIONES COMERCIALES COMO ANTECEDENTE DE LA CONTRATACIÓN POR VÍA ELECTRÓNICA. **III.** OPERACIONES ESTRICTAMENTE NEGOCIALES: LA CONTRATACIÓN ELECTRÓNICA. **1.** Concepto. **2.** El principio de libertad de forma en la doctrina contractualista. **3.** El problema del formalismo indirecto. **4.** Lugar de celebración del contrato electrónico. **IV.** CONTRATOS DOTADOS DE FIRMA ELECTRÓNICA: ASPECTOS LEGISLATIVOS PREVIOS. **1.** La Directiva europea sobre firma electrónica y su transposición al ordenamiento jurídico interno, español e italiano. **1.1.** Evolución legislativa española. **1.2.** Principales normas italianas en materia de firma electrónica. **2.** El nuevo Reglamento europeo sobre identificación electrónica y servicios de confianza para las transacciones electrónicas y su aplicación en España e Italia. **2.1.** Normativa española reguladora de determinados aspectos de los servicios electrónicos de confianza. **2.2.** Adaptación legislativa italiana a la reciente modificación normativa comunitaria.

## I. NATURALEZA JURÍDICA DEL DOCUMENTO: UN LASTRE HEREDADO

Un siguiente paso en nuestro estudio exige analizar la naturaleza jurídica del contrato como soporte de derechos y obligaciones articulado por medios digitales. Ello supone considerar, como elemento matriz, la figura del *documento*[218], que servirá de fundamento primero

[218] El término documento encuentra su origen entre los griegos: el prefijo *dék* viene de *dékos*, que se refiere a un gesto de la mano que se hacía para recibir u ofrecer, fundamentalmente en manifestaciones de carácter religioso. Posteriormente, los latinos retoman la expresión bajo el vocablo *docere*, que se traduce como aquello

con el que poder probar, en su caso, la existencia de la relación contractual, la identidad de los sujetos que en ella intervengan y la integridad misma de su contenido[219].

1. Teoría dualista tradicional: mismos problemas, distinto enfoque

El diccionario de la RAE define el término *documento*, en la segunda de sus acepciones, como «[e]scrito en el que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo»[220]. El término *escrito* procede del infinitivo *escribir*, que viene a significar la representación de palabras o ideas con letras u otros signos trazados en papel u otra superficie (primera acepción), siendo las *letras* cada uno de los signos gráficos que componen el alfabeto de un idioma (primera acepción) y los *signos* los objetos, fenómenos o acciones materiales que, por naturaleza o convención, representan o sustituyen a otro (primera acepción). A su vez, por *dato* se entiende la «[i]nformación sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho» (primera acepción) o, en términos informáticos, la «[i]nformación dispuesta de manera adecuada para su tratamiento por una computadora» (tercera acepción). Por último, *soporte* será aquel «[m]aterial en cuya superficie se registra información, como el papel, la cinta de vídeo o el disco compacto» (cuarta acepción).

De todo ello, y superando los errores de concepto existentes, podemos extraer una definición de documento, a los efectos que aquí interesan, como *contenido almacenado en un soporte físico en papel u otro material adecuado que proporciona información, escrita, vista o hablada, fidedigna o relevante sobre hechos con eficacia probatoria o cualquier otro tipo de utilidad jurídica*[221]. Esta afirmación,

---

que se enseña, instruye o informa. Ambos términos pueden traducirse, en consecuencia, por la expresión *mostrar algo a alguien* (JOLY-PASSANT, E., *L'écrit confronté aux nouvelles technologies*, París, Lgdj, 2006, pp. 63 y 68). Para su estudio desde un punto de vista evolutivo, *vid.* DEVIS ECHANDÍA, H., *Teoría general de la prueba judicial*, Buenos Aires, Zavalía, 1970, pp. 496 y ss.

[219] ORTIZ NAVACERRADA, S., *La prueba de documentos en el proceso civil: estudio jurisprudencial*, Alcobendas, Actualidad, 1994, p. 15, hace referencia al hecho de afrontar, desde el principio, el concepto de documento como algo fundamental y no como una cuestión meramente retórica o académica. En la misma línea, ELÍAS BATURONES, J. J., *La prueba de documentos electrónicos en los tribunales de justicia*, Valencia, Tirant lo Blanch, 2008, p. 1.

[220] Definición inadecuada por cuanto identifica el documento con el registro escrito, de un lado, y el documento con el soporte en que está recogido, de otro.

[221] Elaboración propia.

aparentemente sencilla, ha sido objeto de controversia a lo largo de la historia, dando lugar a debates que, como no, han tenido también su reflejo en distintos textos que, de alguna u otra manera, proceden a regular los efectos jurídicos derivados del documento. Resultado de lo anterior, podemos destacar la existencia de dos teorías, fundamentales, en torno a la configuración del documento desde un punto de vista legal: la *teoría estricta o del escrito* y la *teoría de la representación*. Ambas serán, a lo largo del tiempo, objeto de un profundo estudio, tanto doctrinal[222]como jurisprudencial[223].

La conocida como *teoría estricta*, *del escrito*, *restringida* o *latina*, sostiene que el documento siempre ha de constar por escrito en soporte físico y el soporte físico en papel, identificando, en mi opinión erróneamente, estos términos como sinónimos o equivalentes[224] (**anexo VII**). En esta línea se ubican distintos autores que, de forma patente pero implícita, inciden en esta

[222] Entre los autores que se han pronunciado respecto de esta cuestión, destacan, entre otros, ALMAGRO NOSETE, J., *Derecho procesal*, Valencia, Tirant lo Blanch, 1996, pp. 85 a 91; CARRASCOSA LÓPEZ, V., «Valor probatorio del documento electrónico», *Informática y Derecho: revista iberoamericana de Derecho informático*, vol. 8, 1995, pp. 138 y 139, 147 a 164; MONTERO AROCA, J., *La prueba en el proceso civil*, Madrid, Civitas, 2001, p. 200.

[223] De esta dicotomía se hace eco también la jurisprudencia de nuestro país, como muestra la STS núm. 293/1994, de 24 de marzo, F. J. 2º, cuando, en relación con el término *documento*, diferencia entre «[…] la clásica doctrina que le reputa como sinónimo de escrito a través del cual se exterioriza una idea, pensamiento, convención, negocio jurídico, etc., el cual parece ser se estimó por el legislador procesal de 1881 y no tan exactamente por el civil de 1889, en los artículos 596 y 602 aquél y en los (*artículos*) 1216 a 1230 éste» y lo que «[…] la doctrina procesalista actual califica de funcional, a virtud del cual el concepto de documento ofrece una mayor amplitud en cuanto referido al medio u objeto a través del cual se manifiesta ese pensamiento, idea, etc. –cintas de película o vídeo, estatuas, discos, etc.–, lo que viene en cierto modo amparado por el artículo 1215 CC (*derogado tras la D. D. Única. 2.1 LECiv –BOE núm. 7, de 8 de enero de 2000–*), al emplear el término "instrumentos" en lugar del de "documentos", y que tiene su proyección jurisprudencial entre otras en la Sentencia de esta Sala de 24 de febrero 1956, en la que se concede el carácter de documento a un modelo de cerradura incorporado a los autos, o en la Sentencia de la Sala Sexta (hoy 4.ª) del TS de 5 de julio 1984, que amparada precisamente en el término "instrumentos" del citado artículo 1215 CC, admite como prueba documental la grabación de imágenes de vídeo; o la Sentencia del TC número 190/1992 de 16 noviembre y la en ella citada número 128/1988, de 27 de junio, que estiman "no puede negarse valor probatorio a las transcripciones de una cinta magnetofónica, cuando han sido incorporadas a los autos, no han sido impugnadas y se dan por reproducidas en el acto del juicio oral"» (la cursiva es propia).

[224] Sobre el carácter histórico de esta postura, *vid.* DEVIS ECHANDÍA, H., *Teoría general de la prueba judicial*, cit., pp. 496 y 497.

concepción restringida: así sucede con ÁLVAREZ SAAVEDRA[225], para el que documento no es sino un «[e]scrito con que se prueba, confirma o se hace constar alguna cosa»; ELOSUA DE JUAN[226], que lo concibe como «[i]nstrumento escrito que ilustra sobre algún hecho», añadiendo su gran importancia jurídica como plasmación de declaraciones de voluntad y como medio de prueba de las mismas, o DE LA OLIVA SANTOS[227], que por documento entiende aquellos «[…] objetos materiales que incorporan la expresión escrita de un pensamiento humano y son susceptibles de incorporarse a unos autos o a un expediente». A la vista de lo anterior, jurídicamente, será documento todo escrito (archivado en soporte físico papel) en el cual consta la narración y las circunstancias de uno o más hechos que constituyen, modifican o extinguen relaciones de Derecho entre dos o más personas.

Esta concepción primigenia de documento se fundamenta en el desconocimiento absoluto que, por aquel entonces, existía respecto de los progresos tecnológicos que, posteriormente, se implantarán de manera incuestionable en nuestra sociedad, determinando que distintos cuerpos legales de la época incurran siempre en esta identidad equivocada de vocablos. En concreto el CC[228] y la ALECiv[229], que emplean siempre la palabra *escrito* (en lugar de la expresión, más adecuada en ese momento, de *soporte físico papel*), sin advertir por aquellos tiempos que no todos los documentos tendrán un contenido escrito y que no sólo los documentos en soporte físico papel se servirán de la escritura como medio de representación de la palabra o de la idea.

---

[225] ÁLVAREZ SAAVEDRA, F. J., *Diccionario de criminalística. Los secretos de las investigaciones de la policía científica*, Barcelona, Planeta, 2003, pp. 246 y 247.

[226] ELOSUA DE JUAN, M., *Diccionario LID. Comunicación y marketing*, Madrid, Lid, 2004, p. 137.

[227] DE LA OLIVA SANTOS, A., *Derecho procesal civil*, Madrid, Centro de estudios Ramón Areces, 1995, p. 359. Este mismo autor alude, asimismo, a la necesidad del escrito (concebido erróneamente) en el concepto de documento, afirmando que la voluntad de expandir dicho concepto a realidades técnicas modernas, entre otras adversidades, llevaría a forzar la noción de prueba documental. En concreto, sostiene que ello supone desnaturalizar no pocos preceptos acerca de la prueba documental, que estaban razonablemente pensados para el concepto de documento como expresión escrita (véase, de nuevo, la confusión existente en el empleo del término) de un pensamiento humano, corporeizada en objeto incorporable a los autos de un proceso.

[228] BOE núm. 206, de 25 de julio de 1889.

[229] BOE núm. 36, de 5 de febrero de 1881.

Una segunda teoría, fruto de la decadencia de la concepción anterior, tiende a negar la exclusividad del (mal entendido) escrito como elemento definitorio del documento, concibiendo a este como todo contenido que ofrezca información, más allá del soporte físico y del registro en el que se contenga (**anexo VIII**). Es la conocida como *teoría de la representación* o *germánica*, predominante a partir del momento en el que irrumpen con fuerza los avances propiciados por el mundo digital, que obligan a reconsiderar la idea de documento y a proyectarlo como un concepto ciertamente más amplio.

El origen de esta teoría se encuentra en la distinción, efectuada por CARNELUTTI[230], entre *fuentes de prueba* y *medios de prueba*. Según la misma, y partiendo del hecho de que el fenómeno probatorio no pertenece en exclusiva al mundo jurídico, podemos diferenciar entre *fuente de prueba*, que es un concepto metajurídico, extrajurídico o ajurídico que corresponde a una realidad anterior y extraña al proceso, y *medio de prueba*, que, por el contrario, es un concepto jurídico y absolutamente procesal. Así, la fuente (lo sustancial y material) existirá con independencia de que se siga, o no, el proceso, mientras que el medio (lo adjetivo y formal) nacerá y se formará en el mismo. De este modo, para poder responder a la cuestión acerca de los elementos con los que poder probar un hecho, es preciso efectuar una separación conceptual entre lo que ya existe en la realidad (fuente) y cómo eso que ya existe en la realidad se aporta al proceso (medio). Consecuencia de lo anterior, aun cuando los medios de prueba sean fijos o *numerus clausus*[231], las fuentes de prueba no lo son, más bien todo lo contrario (*numerus apertus*), ya que pueden venir de múltiples canales[232].

---

[230] CARNELUTTI, F., *La prova civile: parte generale. Il concetto giuridico della prova*, Milán, Giuffrè, 1992, pp. 70 y ss. Sobre el uso de la expresión *fuentes de prueba*, *vid.* BENTHAM, J., *Rationale of judicial evidence: specially applied to English practice*, Londres, Manuscrito, 1827, pp. 124 y ss. Más recientemente, pero esenciales en el desarrollo de la distinción entre fuentes y medios de prueba, *vid.* MONTERO AROCA, J., *La prueba en el proceso civil*, cit., pp. 133, 137 y 138 y SENTÍS MELENDO, S., *La prueba: los grandes temas del Derecho probatorio*, Buenos Aires, Ejea, 1979, pp. 141 y ss.

[231] En la ALECiv, confesión en juicio, documentos públicos y solemnes, documentos privados y correspondencia, libros de los comerciantes que se lleven con las formalidades prevenidas, dictamen de peritos, reconocimiento judicial y testigos (artículo 578). En la LECiv actual, interrogatorio de las partes, documentos públicos, documentos privados, dictamen de peritos, reconocimiento judicial e interrogatorio de testigos (artículo 299.1).

[232] En la misma línea, ELÍAS BATURONES, J. J., *La prueba de documentos electrónicos en los tribunales de justicia*, cit., p. 4.

Buen exponente de esta nueva concepción lo constituye la STS de 3 de noviembre de 1997[233], que, impregnándose de los cambios que se estaban produciendo, advierte que:

> «[…] estamos asistiendo, en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse, ya, en exclusiva, con el papel, como soporte, ni con la escritura, como unidad de significación. El ordenador y los ficheros que en él se almacenan constituyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos mercantiles».

En esta misma línea se sitúan, desde un punto de vista doctrinal, autores como RAMOS MÉNDEZ[234], quien afirma que:

> «Vulgarmente se suele identificar el documento con un escrito. Y, desde luego, los escritos son documentos por antonomasia. Sin embargo, el concepto de documento trasciende al de simple escrito. Este constituye la materia del documento: la escritura en sus diversas formas, la tinta el papel, etc. Pero también existen otras materias que pueden servir de soporte físico a un documento

[233] STS de 3 de noviembre de 1997, F. J. 10º. También la STS núm. 380/1997, de 25 de marzo, F. J. 3º, y, antes incluso, la STS de 5 de febrero de 1988, F. J. 1º, en el que se establece que «[…] [e]l tema, efectivamente importante, ofrece una doble consideración o con mayor precisión un tratamiento a dos niveles, el primero el de la legitimidad de la prueba de grabación magnetofónica de la voz y, complementariamente, el de las circunstancias que han de concurrir, en orden a su validez, si se contesta afirmativamente a la primera cuestión, en la efectiva realización de la misma. I. En orden a esta prueba hay que indicar lo siguiente, con carácter general: 1. Las relaciones de medios probatorios de las leyes de procedimiento no tienen el carácter de exhaustivas en cuanto configuran una ordenación acorde con el momento en que se promulgan. Las innovaciones tecnológicas -el cine, el vídeo, la cinta magnetofónica, los ordenadores electrónicos, etc.- pueden y deben incorporarse al acervo jurídico procesal en la medida en que son expresiones de una realidad social que el Derecho no puede desconocer. 2. Todavía más, de alguna manera dichos medios técnicos pueden subsumirse en el concepto mismo amplio, desde luego de documento en cuanto cosas muebles aptas para la incorporación de señales expresivas de un determinado significado», afirmación, esta última, que no impedirá, como veremos, que, años después, la LECiv actual no los incorpore como tal en el elenco del artículo 299.1.

[234] RAMOS MÉNDEZ, F., *Enjuiciamiento civil*, Vallirana, Bosch, 1997, p. 356. También, entre otros, DAVARA RODRÍGUEZ, M. Á., «El documento electrónico, informático y telemático y la firma electrónica», *Actualidad informática Aranzadi: revista de informática para juristas*, vol. 24, 1997, pp. 7 a 13; DE ROSELLÓ MORENO, R., *El comercio electrónico y la protección de los consumidores*, cit., pp. 38 y ss.; DÍAZ FRAILE, J. M., «El documento electrónico y la firma digital: su regulación en la Unión Europea», cit., pp. 9 y ss.; MORENO NAVARRETE, M. Á., *Contratos electrónicos*, Madrid, Marcial Pons, 1999, pp. 90 y ss.

y cada vez con mayor amplitud: cintas magnetofónicas, películas, fotografías, esculturas, fichas o discos de ordenador, ficheros electrónicos, etc. Incluso, elementos que suponen mayores dificultades de traslado físico: inscripciones en monumentos, lápidas conmemorativas, etc.».

También GÓMEZ DE LIAÑO GONZÁLEZ[235] cuando sostiene que:

«Documento, es fundamentalmente un escrito que contiene una declaración de voluntad o de conocimiento, o simplemente una expresión de pensamiento. Suele relacionarse con la idea de escritura porque tradicionalmente era de manera casi exclusiva la forma de contratación. Sin embargo, en el momento presente, las fotografías, películas, discos de ordenador, etc., sirven para incorporar habitualmente una serie de datos que tienen trascendencia en el mundo jurídico, habiendo en este punto quedado atrás la legislación procesal, superada por el avance de los tiempos».

En mi opinión, el problema de este nuevo enfoque, además de su excesiva amplitud, es que incurre en el mismo error que la teoría anterior, ya que, de nuevo, identifica generalmente (en este caso, para proclamar su ampliación) *documento* con *soporte físico papel* y *soporte físico papel* con *escrito*, además de confundir el soporte del documento con la naturaleza de la información que refleja. Sin embargo, no advierte que el nuevo *documento electrónico*, definido en el artículo 3.35) RIE-SCTE como «[…] todo contenido almacenado en formato electrónico, en particular, texto o registro sonoro, visual o audiovisual» y, antes, a nivel nacional, en el artículo 3.5 LFE como la «[…] información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico[236] según un formato determinado[237] y susceptible de identificación y tratamiento diferenciado», puede constar también en soporte físico y por escrito (o, incluso, de manera audiovisual), pero en un material que no es ya el papel, sino otro distinto, apto para el registro de contenido de naturaleza electrónica[238].

---

[235] GÓMEZ DE LIAÑO GONZÁLEZ, F., *El proceso civil*, Oviedo, Forum, 1990, p. 139.

[236] En mi opinión, la redacción de este artículo incurre en un error, ya que confunde el *soporte* (que, aun en el caso del documento electrónico, ha de ser físico) con el *material* de que se componga ese soporte (que en el caso del documento tradicional será el papel, apto para el archivo de información escrita, mientras que en el caso del documento electrónico será uno distinto del papel y apto para el archivo de información escrita, vista o hablada de naturaleza electrónica).

[237] Pero siempre, conviene añadir, de naturaleza electrónica.

[238] También desde una perspectiva puramente doctrinal se ha definido aquello que ha de entenderse por documento electrónico. Entre los autores destaca VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., p. 37, quien entiende por tal «[…] la representación en lenguaje digital o binario, descodificable, referida a hechos o actos

Esta confusión, heredada en el tiempo, constituirá, precisamente, la base doctrinal que, como veremos más adelante, llevará a la LECiv actual a reconocer legalmente a los documentos electrónicos como medio de prueba (artículos 299.2 y 382 a 384), pero, bajo su denominación como *instrumentos*, a sacarlos fuera de la prueba documental (artículos 299.1.2.º y 3.º y 317 a 334)[239].

2. Nueva propuesta: la teoría del documento como contenido y el principio de equivalencia funcional como instrumento reparador

En realidad, lo único que se produce con la irrupción de las nuevas tecnologías de la información y de la comunicación es una ampliación (derivada de la aparición de la electrónica) en la variedad de los materiales de los soportes físicos, capaces, ahora, de albergar, no sólo datos fidedignos o susceptibles de ser empleados como tales para probar algo en forma escrita (definición actual de *documento* contenida en la RAE), sino también en forma vista o hablada, innovación hasta el momento desconocida (y que, por ende, habrá de propiciar la modificación o ampliación de la definición anterior y de cuantas se hallen expresadas en términos similares). Es esta razón la que justifica mi propuesta de dar un paso más, en una nueva teoría que podríamos denominar *teoría del documento como contenido*[240], que amplía la noción de documento, partiendo de la palabra escrita y extendiéndola a la imagen y al sonido, que, ahora sí (a raíz, fundamentalmente, de la promulgación del RIE-SCTE), pueden quedar archivados para su posterior utilización como medio de prueba en un proceso judicial (**anexo IX**). Y todo ello sintetizado en una propuesta de definición de documento que, de nuevo, reproducimos: *contenido almacenado en un soporte físico en papel u otro material adecuado que proporciona información, escrita, vista o hablada, fidedigna o relevante sobre hechos con eficacia probatoria o cualquier*

---

con relevancia jurídica, plasmada en un soporte electrónico con aptitud para su consulta, comunicación o transmisión». Este mismo autor entiende que el documento electrónico se caracteriza por las siguientes notas distintivas: en primer lugar, porque su creación y uso precisa de dispositivos especiales; en segundo lugar, porque están redactados en un lenguaje no convencional; en tercer lugar, porque se incorporan a un soporte especial en continua obsolescencia; en cuarto lugar, por su aptitud para su transmisión y modificación; en quinto lugar, por su relevancia jurídica y, en sexto y último lugar, por su equivalencia funcional en cuanto a la prueba (*Ibid.*, pp. 38 a 40).

[239] GOMES SOARES, F. S., «La prueba en la contratación electrónica de consumo», cit., p. 8; VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, Madrid, Reus, 2005, p. 237.

[240] Precisamente por entender que es este, el contenido, el que define al documento y no el soporte físico (continente) en el que dicho contenido (o documento) se encuentra recogido.

*otro tipo de utilidad jurídica*. Lo importante, por tanto, no es el material (papel o cualquier otro apto para el archivo de la información) del soporte físico en que conste el documento, sino que este (como contenido que plasma información escrita, vista o hablada) sea susceptible de ser empleado como medio de prueba en juicio y de acompañarse, a su vez, de otros tantos medios, como la firma electrónica, que aporten seguridad adicional en cuanto a la existencia de la relación jurídica, a la identificación del/de los autor/es del documento y a la integridad misma de la información que plasma.

Esta teoría se ve reforzada por la definición que del término *documento* se contiene en diversos sectores de nuestro sistema jurídico nacional. Así sucede, en primer lugar, con el artículo 49.1 LPHE[241], que entiende por documento «[…] toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes[242] informáticos»; como podemos observar, bajo la cobertura de esta Ley se incluiría todo tipo de documento, con información escrita, visual o sonora, que conste en soporte papel o cualquier otro idóneo a los fines expuestos, expandiendo la noción de documento de forma paralela al desarrollo de los nuevas tecnologías. En segundo lugar, el artículo 76.3, *in fine*, RITPAJD[243], que hace lo propio cuando, aun de manera más restringida (no contempla el documento aportando información de naturaleza distinta a la escrita), afirma que por documento se entenderá «[…] cualquier soporte[244] escrito, incluidos los informáticos, por los que se pruebe, acredite o se haga constar alguna cosa»; vemos cómo, aquí, sí se incluye el escrito como cualidad también posible de los documentos electrónicos, haciendo mención, además, a la finalidad probatoria que estos están llamados a cumplir. En tercer y último lugar se encuentra el artículo 26 CP[245], que, al definir el documento como «[…] todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica», incurre en el error de identificar el contenido (documento) con el continente (soporte material) pero proporciona una definición general abierta a todo tipo de soportes (papel o cualquier otro adecuado,

[241] BOE núm. 155, de 29 de junio de 1985.

[242] Mejor dicho, *los soportes físicos distintos del papel pero aptos para el archivo de información de naturaleza electrónica.*

[243] BOE núm. 148, de 22 de junio de 1995.

[244] Mejor dicho, *cualquier soporte físico que albergue en su interior información escrita.*

[245] BOE núm. 281, de 24 de noviembre de 1995.

presente o futuro) en que dicho documento se pueda hacer constar, siempre que hagan que este tenga relevancia probatoria o cualquier otra utilidad de naturaleza jurídica.

También interesa destacar en este punto el artículo 9.1 DCE y, tanto más, el artículo 23.1 y 3 LSSICE, que tratan de solventar el problema, heredado a lo largo del tiempo, de la errónea identificación entre *documento* y *soporte*, entre *soporte físico y soporte físico papel* y entre *soporte físico papel* y *escrito*. Y lo hacen acudiendo al conocido como *principio de equivalencia funcional*, que se basa en la posibilidad de dar cumplimiento a los requisitos legales de forma mediante el empleo de fórmulas electrónicas adecuadas a los objetivos y funciones a los que tradicionalmente responden[246]. Merced a este principio, la función jurídica que, en toda su extensión,

[246] SCOTTI, L. B., *Contratos electrónicos: un estudio desde el Derecho internacional privado argentino*, cit., p. 57; VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 44 a 46, 74 a 77. A nivel internacional, el principio de equivalencia funcional se recoge por primera vez en la LMACI, cuyo artículo 7.3, a fin de cumplir con el requisito *escrito* sobre el que ha de constar el acuerdo de arbitraje, establece que «[s]e entenderá que el acuerdo de arbitraje es escrito cuando quede constancia de su contenido en cualquier forma, ya sea que el acuerdo de arbitraje o contrato se haya concertado verbalmente, mediante la ejecución de ciertos actos o por cualquier otro medio». Once años después, el artículo 5 LMCE persigue continuar con el fin descrito con la siguiente formulación: «[n]o se denegarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos»; así, como bien explica el apartado 46 de la Guía para la incorporación al Derecho interno de la LMCE, este precepto «[…] se limita a indicar que la forma en que se haya conservado o sea presentada cierta información no podrá ser aducida como única razón para denegar eficacia jurídica, validez o fuerza ejecutoria a esa información», si bien, advierte, ello no debe interpretarse erróneamente «[…] como si fuera un texto por el que se conced[e] validez jurídica a todo mensaje de datos o a todo dato en él consignado». También, posteriormente, y para las comunicaciones electrónicas, el artículo 9, desarrollado en el apartado 51, donde afirma que «[e]l enfoque de la equivalencia funcional se basa en un análisis de los objetivos y funciones del requisito tradicional de que los documentos se consignen en papel con miras a determinar cómo podrían cumplirse estos objetivos y funciones con técnicas de comercio electrónico». Por último, y de manera más reducida, el artículo 13 CNUCCIM (A/35/51), cuando dice que, «[a] los efectos de la presente Convención, la expresión "por escrito" comprende el telegrama y el télex». Lo propio hace, en el ámbito del Derecho comunitario, el artículo 9.1 DCE (desarrollado en el considerando 34), que exige a los Estados miembros que su legislación no obstaculice el desarrollo y utilización de los contratos electrónicos; en concreto, se les pide que modifiquen y adapten su normativa para eliminar cualquier tipo de traba (especialmente los requisitos formales, incluido el registro de la contratación) que pueda entorpecer la celebración de contratos por vía electrónica en cualquiera de sus fases, apostando decididamente a favor de la existencia y validez de los mismos. La eficacia de esta previsión se vería reforzada al eliminarse los problemas relativos a la autoría, integridad y confidencialidad de los datos, a través de la legislación contenida en el RIE-SCTE, cuyo artículo 46 prohíbe la denegación de efectos jurídicos y de admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero

vendría a cumplir la instrumentación autógrafa del documento tradicional plasmado en soporte físico papel (también, eventualmente, su expresión oral) en relación con todo tipo de actos jurídicos, podría verse igualmente satisfecha con la instrumentación digital (escrita, visual o sonora) del documento contenido en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica, más allá del alcance y de la finalidad del acto así configurado. Con ello conseguimos, en definitiva, que los efectos jurídicos perseguidos por quien resulte ser el emisor de una declaración de voluntad se vean cumplidos con independencia del soporte en el que conste dicha declaración[247].

No obstante, pese a cumplir el fin para el que fue concebido (como es el de equiparar, dentro de la noción de documento –en este caso en su modalidad de contrato–, al archivado en soporte físico papel y al archivado en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica), el principio de equivalencia funcional contenido en el español artículo 23.3 LSSICE emplea términos, en mi opinión, mejorables: «[s]iempre que la Ley exija que el contrato o cualquier información relacionada con el mismo

---

hecho de estar en formato (o, mejor dicho, soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica) electrónico. Finalmente, el artículo 23.1 y 3 LSSICE recoge en España el principio de equivalencia funcional en materia de contratación electrónica, que no sólo se predica respecto de la celebración misma del contrato, sino, también, en relación a otros deberes relativos a la entrega en forma escrita de determinada información en el marco de la formación o el cumplimiento de este, resultando igualmente concluyente ante eventuales consecuencias administrativas por falta de entrega de determinada información. Esta equiparación queda legalmente formulada para los casos en que una norma exija forma escrita (mejor dicho, soporte físico papel) como requisito de validez y eficacia del contrato, pero también despliega sus efectos en materia probatoria, regulada en el artículo 24.1.1º y 2 LSSICE –sin equivalente en la DCE, sí en la LMCE (artículo 9)–, que, como veremos más adelante, dispone que la prueba de un contrato electrónico, así como la de las obligaciones que en él tengan su origen, se sujetará a las reglas generales del ordenamiento jurídico, añadiendo que el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba de carácter documental. Si, además, se exige que el documento incorpore la firma manuscrita, será preciso acudir al uso de firmas electrónicas para entender satisfecho este requisito, más concretamente a los artículos 25 y ss. RIE-SCTE (también, cuando los documentos electrónicos vayan acompañados de un sello electrónico, de un sello de tiempo electrónico o de un servicio de entrega electrónica certificada, será preciso acudir a los artículos 35 y ss.) y 3 LFE (o, en su caso, al artículo 3 ALSEC, caso de que finalmente el Anteproyecto entre en vigor).

[247] ILLESCAS ORTIZ, R., «La equivalencia funcional como principio elemental del Derecho del comercio electrónico», *Revista Derecho y tecnología*, vol. 1, 2000, p. 11; en la misma línea, PÉREZ PEREIRA, M., *Firma electrónica: contratos y responsabilidad civil*, cit., pp. 81 y 82.

conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico». En concreto, con la redacción actual de la norma, se mantiene el error de concepto y de identificación tantas veces criticado a lo largo de estas líneas, que simplemente se "parchea" para evitar sus perniciosos efectos y para hacer operativa la introducción del desarrollo digital en el ámbito del Derecho por medio de la fórmula, adecuada pero planteada en términos equivocados, de la equivalencia funcional. Así, una redacción de la Ley con fines más ambiciosos podría haber quedado redactada de la siguiente manera[248]:

> *Siempre que la Ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene tanto en soporte físico papel como en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica.*

De este modo, se verían cumplidas las exigencias actualmente contenidas en la normativa para las tradicionales funciones del mal concebido *escrito*, es decir, del documento en soporte físico papel.

En cualquier caso, desde una perspectiva puramente negocial, ello determinará la base que justifica la aparición del contrato electrónico, de modo tal que aquellos contratos perfeccionados mediante el uso de las nuevas tecnologías no podrán tener peor (ni mejor) consideración jurídica que aquellos que sean plasmados por medios convencionales y tradicionales. Se da lugar, así, a lo que se conoce como *principio de no discriminación*[249], que vendría a ser, respecto de la equivalencia funcional, la cara (expresada en términos negativos) de una misma moneda.

3. Elementos esenciales y clasificación actual del documento

Fruto del análisis anterior, cabría esperar que la concepción acerca de los elementos esenciales del documento que, a efectos de validez y eficacia, se ha venido elaborando doctrinal y jurisprudencialmente, se adapte, desde un punto de vista conceptual, a los avances tecnológicos propiciados por la sociedad de la información. Tradicionalmente, estos elementos esenciales se han concretado en torno a los siguientes[250]: en primer lugar, el *soporte físico o*

[248] Elaboración propia.

[249] MADRID PARRA, A., «Instrumentos de la CNUDMI/UNCITRAL sobre comercio electrónico (contratación, firma y comunicaciones comerciales)», cit., pp. 315 y 316.

[250] STS núm. 865/1997, de 13 de junio.

*continente*, en la concepción de documento como contenido recogido en una cosa mueble que puede ser llevada ante el juez a los efectos que resulten procedentes; en segundo lugar, el *acto documentado*, que será el hecho relevante representado en el documento; en tercer lugar, *el/los autor/es del documento*, que serán las personas a las que se atribuya su formación o la asunción del contenido, y, en cuarto y último lugar, *la representación*, donde se habrán de incorporar nociones más amplias de documento que permitan incluir, además de representaciones de hechos mediante escritura, las practicadas por otros medios como la imagen o el sonido.

De ello podemos extraer dos consideraciones importantes. En primer lugar, observamos que, por regla general, el documento no requiere de firma ni de fecha para que sea válido y eficaz, si bien a nadie escapa (y así se hará constar) que ambos elementos constituirán un instrumento ciertamente relevante para la satisfacción del fin probatorio que todo documento, sea de la naturaleza que sea, puede tratar de satisfacer[251]. En segundo lugar, a la vista de lo anterior, la asunción legal del concepto en los términos expuestos no obstaculizaría de ninguna manera el cumplimiento de las funciones propias de todo documento, que se resumen en las siguientes[252] (**anexo X**): función *perpetuadora*, en cuanto fijación material y perdurable de manifestaciones del pensamiento; función *garantizadora*, en cuanto sirve para asegurar que la persona identificada en el documento es la misma que ha realizado las manifestaciones que se recogen en el mismo[253] y, en último lugar, función *probatoria*, en cuanto acreditación o prueba de un hecho concreto. Esta última, a su vez, cumplirá una función *indicativa*, pues permitirá individualizar e identificar al autor del documento, principalmente si es manuscrito o está firmado; una función *declarativa*, que consistirá en la asunción de la paternidad del documento por parte de su autor, y una función *probatoria propiamente dicha*, que posibilitará la adveración de la autenticidad del documento.

---

[251] MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., p. 129; PLAZA PENADÉS, J., «La firma electrónica (regulación en España y en la Unión Europea)», en PLAZA PENADÉS, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, p. 413; VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., p. 123; VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», *Revista de estudios económicos y empresariales*, vol. 23, 2011, p. 137.

[252] TOSI, E., *Il contratto virtuale*, Milán, Giuffrè, 2005, p. 269; VEGA VEGA, J. A., «El documento jurídico. Problemas de la electronificación», *Revista de estudios económicos y empresariales*, vol. 25, 2013, pp. 160 a 166; VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 48 a 52.

[253] STS núm. 865/1997, F. J. 3º.

A su vez, podemos establecer distintas clasificaciones, actualmente válidas, de documento, atendiendo a criterios varios que podrán, o no, darse cumulativamente en un mismo supuesto[254] (**anexo XI**):

En primer lugar, por el origen, podemos distinguir entre *documento público* y *documento privado*[255]. El documento público es aquel realizado por un funcionario público en el desempeño de sus funciones. Dentro de él, podemos hablar, a su vez, de *documento oficial* y *documento público propiamente dicho*, ambos provenientes de sujetos que desempeñan una función pública, si bien, en este último, la persona tiene encomendada específicamente la función de dar fe pública sobre el contenido del documento. En nuestro país, el artículo 1216 CC define los documentos públicos como aquellos «[…] autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la ley». Asimismo, de acuerdo con el artículo 317 LECiv, a efectos de prueba en el proceso, se considerarán documentos públicos: 1) las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Secretarios Judiciales, 2) los autorizados por Notario con arreglo a Derecho, 3) los intervenidos por Corredores de Comercio colegiados y las certificaciones de las operaciones en que hubiesen intervenido, expedidas por ellos con referencia al libro registro que deben llevar conforme a Derecho, 4) las certificaciones que expidan los Registradores de la Propiedad y Mercantiles de los asientos registrales, 5) los expedidos por funcionarios públicos legalmente facultados para dar fe en lo que se refiere al ejercicio de sus funciones y 6) los que, con referencia a archivos y registros de órganos del Estado, de las Administraciones públicas o de otras entidades de Derecho público, sean expedidos por funcionarios facultados para dar fe de disposiciones y actuaciones de aquellos órganos, Administraciones o entidades. En su vertiente puramente virtual, el artículo 3, apartados 5 y 6, LFE, vino a complementar a los preceptos anteriores otorgando, por primera vez, reconocimiento legal a la figura del documento público electrónico, poniendo fin a la discusión abierta sobre su posible existencia a efectos jurídicos[256] y realizando una separación entre aquellos documentos pú-

[254] MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., pp. 243 a 245; VEGA VEGA, J. A., «El documento jurídico. Problemas de la electronificación», cit., pp. 166 a 172.

[255] VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., pp. 137 y 138.

[256] PLAZA PENADÉS, J., «Eficacia de la firma electrónica en los Registros de la Propiedad y Mercantil», *Revista crítica de Derecho inmobiliario*, vol. 667, 2001, p. 2038, señalaba, ya en su momento, que «[…] nada impide que un

blicos firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso –letra a) del artículo 3.6 LFE–, y aquellos otros expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica –letra b) del artículo 3.6 LFE–.

Por su parte, los documentos privados serán aquellos realizados por un particular o persona privada, siendo definidos, en sentido negativo, por el artículo 324 LECiv como «[…] aquellos que no se hallen en ninguno de los casos del artículo 317». Consecuencia de lo anterior, serán documentos privados aquellos que no sean documentos públicos[257].

En segundo lugar, por el continente en que se encuentra recogido el documento, y fruto de la irrupción del elemento virtual en el análisis de la realidad actual, hablaremos de *soporte físico papel* y de *soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica.*

En tercer lugar, por la naturaleza jurídica propia del documento, a los efectos que aquí nos interesan, cabría diferenciar entre *documentos expresivos de contratos* y *documentos no expresivos de contratos*. Un documento contractual sería aquel que refleja la oferta por el vendedor, la aceptación por el destinatario, las condiciones generales de la contratación que afectan a la relación negocial o, conjuntamente, el contenido y el consentimiento de las partes en obligarse recíprocamente.

En cuarto lugar, según el documento esté, o no, refrendado por su autor o por la persona que lo acepta, estaremos ante un *documento firmado* o ante un *documento no firmado*. Asimismo, el documento firmado, según se trate de documento recogido en soporte físico papel o en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica, estará refrendado por una firma manuscrita o por una firma electrónica, firma electrónica que, además, podrá presentar distintos niveles de seguridad, según se trate de firma

documento electrónico pueda revestir el carácter de público si es emitido por un Notario o empleado público competente, con las solemnidades requeridas por la ley, cuando desempeña su función legal de fedatario o funcionario público».

[257] BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», *Foro: revista de ciencias jurídicas y sociales*, vol. 3, 2006, pp. 450 y 451.

electrónica simple, avanzada o cualificada. Como decíamos antes, este requisito no afecta a la validez o eficacia del documento (en este caso del contrato), que podrá existir aun sin venir acompañado de firma, en cuyo caso podremos llegar a determinar su autoría o integridad acudiendo a otros medios de prueba de los contemplados en el artículo 299 LECiv[258]. Pese a ello, es obvio que, a los efectos de imputar su contenido a una persona determinada, la firma juega un papel esencial: si estamos ante un documento tradicional, la firma manuscrita servirá para presumir la autoría y la aceptación de cuanto en él se expresa por quien aparece como firmante o signatario, si bien se tratará de una presunción *iuris tantum* que podrá ser rebatida acudiendo, por ejemplo, a una prueba caligráfica; si estamos ante un documento electrónico, la firma electrónica (dependiendo del nivel de seguridad que ofrezca) podrá determinar la paternidad del documento del mismo modo que la firma manuscrita, además de su integridad y no rechazo (o no repudio), no sirviendo para rebatirla, al menos íntegramente, los mismos medios que para la firma tradicional.

Por último, en atención a su valor probatorio, estaremos ante *documentos que constituyen prueba plena en juicio*, que serán los del artículo 299.1 LECiv, y *documentos que serán valorados conforme a las reglas de la sana crítica*, contenidos en los apartados 2 y 3 de dicho precepto.

## II. COMUNICACIONES COMERCIALES COMO ANTECEDENTE DE LA CONTRATACIÓN POR VÍA ELECTRÓNICA

En el ámbito del comercio electrónico, al igual que sucede con el comercio tradicional, la formación del contrato suele ir precedida de una cierta actividad publicitaria. Es habitual que la oferta de contrato o las invitaciones a contratar sean la prolongación de una previa, pero no obligatoria, labor comercial. De este modo, los grandes principios que informan el Derecho de la contratación electrónica disciplinan también la etapa precontractual, dominada decisivamente por la actividad publicitaria[259].

Como es lógico, la publicidad, tanto en el mundo físico como en el mundo virtual, se halla sometida a una serie de normas que rigen su funcionamiento, sin que los distintos soportes utilizados supongan diferenciación alguna al respecto: a las mismas reglas se somete el *banner*

[258] MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», en PEGUERA POCH, M. (coord.) *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010, p. 224.

[259] ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., p. 243.

insertado en una página web que el mensaje publicitario contenido en la edición en papel de un periódico. En un plano europeo e interno español, los artículos 6 a 8 DCE y 19 a 22 LSSICE, respectivamente, establecen que las comunicaciones comerciales electrónicas englobarán todas aquellas formas de comunicación destinadas a promocionar[260], ya sea directa o indirectamente, los bienes, servicios o imagen de una empresa, organización o persona que realiza una actividad comercial, industrial, artesanal o profesional[261] –letra f) del artículo 2 DCE y letra f) del anexo LSSICE–[262]. Serán, por tanto, SSI que, representando una actividad económica, directa o indirecta, para el PSSI, no son remunerados por los DSSI (considerando 18 DCE y apartado II de la Exposición de Motivos de la LSSICE).

Desde una perspectiva comunitaria, el artículo 6 DCE establece los requisitos que habrán de cumplir las comunicaciones comerciales para poder ser válidas a efectos jurídicos. Estos requisitos serán, de forma resumida, los siguientes: en primer lugar, que sean claramente identificables como tales, no pudiendo ocultarse bajo otro nombre distinto que induzca a error a quien las recibe; en segundo lugar, que se identifique con exactitud la persona, física o jurídica, en nombre de la cual se envían tales comunicaciones comerciales, y, en tercer lugar, que se detallen con precisión las ofertas promocionales y los concursos o juegos promocionales de que, en su caso, se hagan acompañar[263], siempre que estén permitidos en el Estado miembro en que esté establecido el PSSI, sean fácilmente accesibles y se presenten de manera clara e inequívoca las condiciones que han de cumplirse para poder obtenerlos.

---

[260] El artículo 2.f) DCE emplea, entiendo que por error, el término *proporcionar* en lugar del de *promocionar*.

[261] A las comunicaciones comerciales se refiere el considerando 29 DCE, que destaca el papel esencial que estas juegan a la hora de financiar los SSI y el desarrollo de una amplia variedad de servicios nuevos y gratuitos.

[262] No tendrán la consideración de comunicaciones comerciales en sí mismas ni los datos que permitan acceder de manera directa a la actividad de la empresa, organización o persona (nombre de dominio o dirección de correo electrónico) ni aquellas comunicaciones concernientes a los bienes, servicios o imagen de la empresa, organización o persona en aquellos casos en que sean elaboradas por un tercero de forma independiente, ajena y sin contraprestación económica alguna.

[263] El considerando 16 DCE explica cómo la exclusión de las actividades relacionadas con los juegos de azar del ámbito de aplicación de la Directiva se refiere, tan sólo, a juegos de azar, loterías y apuestas que impliquen una participación con valor monetario –de ahí el artículo 1.5.d) DCE–. No abarca, pues, a los concursos o juegos promocionales que tengan por objeto fomentar la venta de bienes o servicios y en los que los pagos, de haberlos, tan sólo sirven para adquirir aquellos.

Una de las cuestiones más problemáticas viene determinada por el envío masivo e indiscriminado de comunicaciones comerciales virtuales de carácter publicitario o promocional por correo electrónico u otro medio equivalente que, con carácter previo, no hayan sido solicitadas o expresamente autorizadas por los destinatarios de las mismas (actividad, esta, conocida como *spamming*[264]).

Su tratamiento legal (artículo 7 DCE[265]) constituye una innovación específica del Derecho de la contratación electrónica y una excepción al principio de inalterabilidad del Derecho preexistente, ya que supone la creación de una nueva regla para un hecho hasta ahora prácticamente desconocido y sin paralelismo en el mundo de la publicidad en formato físico, motivado, entre otras cosas, por el escaso o nulo coste que supone para quien los envía[266]. El núcleo de esta normativa se centra en determinar tres aspectos básicos: la admisibilidad (o no) del empleo de los datos personales de los DSSI, la necesidad (o no) de consentimiento previo y la existencia (o no) de un derecho de exclusión[267]. En este sentido, dos han sido, tradicionalmente, las opciones de política legislativa en orden a establecer la licitud o ilicitud de las comunicaciones comerciales no solicitadas: una primera, que agrupa a los denominados sistemas *opt-out*, que permite enviar mensajes publicitarios no solicitados a todos los destinatarios que no hayan optado por no recibirlos, habiendo de dar al receptor la posibilidad de exigir que no se le envíen nuevos mensajes; una segunda, que engloba a los denominados sistemas *opt-in*, donde el mensaje publicitario sólo es lícito si, con anterioridad, el destinatario ha optado por recibir comunicaciones comerciales, de modo que no es suficiente con no

[264] Más conocido popularmente como *correo basura*, el *spamming* se presenta, desde un punto de vista teórico, como una violación de la intimidad, de la privacidad y de los más elementales derechos de la propiedad privada. Su control o seguimiento presenta dificultades patentes, derivadas de las propias características inherentes a su naturaleza, al igual que su regulación jurídica, ya que prohibirlo por completo puede suponer la configuración de una legalidad de difícil cumplimiento práctico. Sobre esta cuestión, *vid.* DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 256.

[265] El texto del artículo 7 DCE puede inducir a error, ya que en este apartado se hace referencia a aquellas comunicaciones comerciales por correo electrónico no solicitadas, no a las comunicaciones comerciales no solicitadas por correo electrónico.

[266] ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., p. 244.

[267] PEGUERA POCH, M. Y OTROS, «Marco jurídico de los servicios de la sociedad de la información y del comercio electrónico», cit., pp. 362 y 363

oponerse (sistema *opt-out*), sino que ha de existir una solicitud expresa o un rechazo palmario a su envío[268].

La DCE opta por la primera modalidad, imponiendo, además de otros requisitos establecidos en el Derecho comunitario, que los Estados miembros que permitan las comunicaciones comerciales enviadas por PSSI establecidos en su territorio y no solicitadas por los DSSI, garanticen que estas sean, clara e inequívocamente, identificables como tales en el mismo momento de su recepción, no redundando en gastos suplementarios para el receptor. Adicionalmente, se pide a tales Estados que, sin perjuicio de lo dispuesto en la DPCCD[269] y en la DTDP, adopten cuantas medidas sean necesarias para garantizar que los PSSI que realicen estas comunicaciones comerciales no solicitadas consulten regularmente, primero, y respeten, después, las listas de exclusión voluntaria[270] en las que se podrán inscribir las personas físicas que no deseen recibir dicha publicidad. Ahora bien, ¿por qué sólo las personas físicas pueden solicitar esta exclusión y no también las personas jurídicas? La razón estriba, entiendo, en la protección adicional que merecen aquellos individuos que, en su condición de consumidores, utilizan un SSI en el marco de una actividad no profesional; en cambio, las personas jurídicas (que, recordemos, pueden actuar, o no, en el marco de una actividad profesional a la hora de utilizar un SSI) no se encuentran en esa situación desfavorable y digna de protección reforzada, manteniéndose al margen de ese derecho de rechazo. Pese a ello, y aun siendo ese el motivo, con esta previsión normativa se establece una notoria discriminación entre las personas jurídicas que actuarían en el marco de su actividad profesional (que se ven impedidas a la hora de inscribirse en las listas de exclusión voluntaria de comunicaciones comerciales no solicitadas) y las personas físicas que, al igual que las anteriores, actúan en el ámbito de su profesión o negocio a la hora de utilizar un SSI (y que, pese a no encontrarse tampoco en esa situación desfavorable y ávida de protección, sí que cuentan con el precitado derecho).

---

[268] FINOCCHIARO, G. D. Y OTROS, *Diritto dell'informatica*, cit., p. 36.

[269] DOCE L 144, de 4 de junio de 1997, p. 19. Esta Directiva se ha visto sucesivamente modificada por la DCDSFDC (DOCE L 271, de 9 de octubre de 2002, p. 16), por la DPCD (DOUE L 149, de 11 de junio de 2005, p. 22) y por la DSPMI (DOUE L 319, de 5 de diciembre de 2007, p. 1).

[270] En España, este servicio, gestionado por la Asociación Española de la Economía Digital, es conocido tradicionalmente como *Lista Robinson*.

Por último, el artículo 8 DCE regula el supuesto del uso de comunicaciones comerciales que, en todo o en parte, constituyan un SSI facilitado por un miembro de una profesión regulada[271], supuesto este en el que esta norma será de aplicación conjunta con el resto de directivas comunitarias relativas al acceso a las actividades de las profesiones reguladas y a su ejercicio, «manteniendo un conjunto coherente de normas aplicables en la materia». En estos casos, se impone a los Estados miembros que garanticen la posible utilización de la publicidad, si bien estará condicionada al cumplimiento de normas profesionales relativas, en particular, a la independencia, a la dignidad, al honor, al secreto profesional y a la lealtad, tanto a los clientes como a los colegas. A fin de determinar la información que pueda facilitarse en estas comunicaciones comerciales, los Estados miembros y la Comisión fomentarán, sin perjuicio de la autonomía de los colegios y asociaciones profesionales, que estos establezcan códigos de conducta comunitarios[272].

---

[271] Este artículo no cuenta con su equivalente en la LSSICE, de modo que se entiende extensivo y directamente aplicable al uso de comunicaciones comerciales que, íntegra o parcialmente, constituyan un SSI facilitado por un miembro de una profesión regulada (y, por ende, PSSI) al que le resulte de aplicación la normativa española.

[272] En estos casos, la Comisión no sólo fomentará esta actuación, sino que, cuando tenga que elaborar propuestas de iniciativas comunitarias que puedan resultar necesarias para garantizar el funcionamiento adecuado del mercado interior en lo que se refiere a la información que puede facilitarse a efectos de comunicaciones comerciales que, en todo o en parte, constituyan un SSI, tendrá debidamente en cuenta tales códigos de conducta y actuará con colegios y asociaciones profesionales en estrecha cooperación (considerandos 32 y 33 DCE). Además, la Comisión, con objeto de que los SSI adquieran una mayor difusión apoyándose en tecnologías fiables, seguras y dignas de confianza, ha procedido a regular sobre la materia; fruto de esta labor, tuvo lugar la CCLCS –COM (2006) 688 final–, donde la Comisión indica algunas medidas nuevas que podrían adoptarse respecto de estos problemas, en particular, la represión de las actividades ilícitas, el fortalecimiento del Derecho comunitario, la cooperación dentro de los Estados miembros, el fomento de las actividades de investigación y desarrollo, el diálogo político y económico con terceros países o la puesta en práctica de iniciativas dentro del sector, poniendo de manifiesto, además, que el correo electrónico no solicitado, simple molestia en un principio, ha pasado en la actualidad a convertirse en fuente de actividades fraudulentas y delictivas, como es el caso, en especial, del *phising*, que induce a los usuarios a facilitar datos sensibles a través de páginas web que imitan las de las empresas auténticas, dando lugar a supuestos de falsificación de la identidad y a patentes perjuicios a la buena reputación de las empresas. La difusión de programas maliciosos, como virus y gusanos, también facilita el envío masivo de correos electrónicos no solicitados, programas que, una vez instalados, permiten al atacante hacerse con el control de un sistema informático infectado y convertido en un *botnet*, convirtiendo a esos ordenadores en servidores de correo sin que lo sepan sus usuarios, por medio de la ocultación de la identidad del verdadero emisor del *spam*. Para un estudio más profundo de todo cuanto tiene que ver con esta cuestión, *vid.* DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 257.

En un plano interno, la LSSICE regula esta cuestión, como decíamos, en los artículos 19 a 22. El primero de estos preceptos establece la aplicación conjunta de esta Ley junto con toda la normativa vigente en materia comercial y de publicidad[273], habiendo de tener en cuenta, en todo caso, la LOPDCP[274], así como su normativa de desarrollo[275], en especial en todo aquello concerniente a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

Por su parte, el artículo 20 LSSICE, siguiendo la estela del artículo 6 DCE, exige que las comunicaciones comerciales electrónicas, al igual que la persona física o jurídica en nombre de la cual se lleven a cabo, sean claramente identificables[276]. Claramente reconocibles deberán

[273] De este modo, serán de aplicación, además de las normas generales sobre la materia, contenidas fundamentalmente en la LGP (BOE núm. 274, de 15 de noviembre de 1988), el artículo 61 TRLGDCU, que reglamenta la integración de la oferta, la promoción y la publicidad en el contrato, estableciendo, en su apartado primero, que todas ellas «[…] se ajustarán a su naturaleza, características, utilidad o finalidad y a las condiciones jurídicas o económicas de la contratación», a lo que añade (apartado segundo) que «[e]l contenido de la oferta, promoción o publicidad, las prestaciones propias de cada bien o servicio, las condiciones jurídicas o económicas y garantías ofrecidas serán exigibles por los consumidores y usuarios, aun cuando no figuren expresamente en el contrato celebrado o en el documento o comprobante recibido y deberán tenerse en cuenta en la determinación del principio de conformidad con el contrato». Ahora bien, si el contrato celebrado contuviese cláusulas más beneficiosas, estas se impondrán sobre el contenido de la oferta, promoción o publicidad (apartado tercero). También el artículo 94 TRLGDCU, que dispone que, cuando su contenido entre en contradicción con el contenido de la normativa específica sobre SSI y comercio electrónico, «ésta será de aplicación preferente, salvo lo previsto en el artículo 97.7.2º TRLGDCU».

[274] BOE núm. 298, de 14 de diciembre de 1999.

[275] Fundamentalmente, el RDRDLOPDCP (BOE núm. 17, de 19 de enero de 2008).

[276] En palabras de ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 243 y 244, «[s]i en algo se altera el Derecho preexistente en la materia lo es para insistir en la vigencia reforzada de la vieja regla de la autenticidad publicitaria hoy desaparecida, en su formulación directa, de aquella LGP. Por así decir, la regla de autenticidad publicitaria reaparece para el comercio electrónico, en cuya esfera se hace obligatoria la identificación del mensaje publicitario. Así, el artículo 20.1 de la LSSICE […]». No obstante, añade, «[s]emejante exigencia resulta fácilmente eludible cuando el iniciador del mensaje –publicitario y de datos– carente de identificación goza de extraterritorialidad, lo que resulta tan frecuente en el comercio electrónico. Se trata además de una exigencia que respecto del comercio entre empresarios ni goza de fundamento en el Derecho comunitario europeo ni en la inalterabilidad del Derecho preexistente; en la materia, precisamente […], la autenticidad publicitaria perdió su reconocimiento legal y a lo sumo la misma puede entenderse como un mero subproducto del principio de

ser también las distintas ofertas promocionales (tales como descuentos, premios y regalos), concursos o juegos promocionales, que, previa la correspondiente autorización, deberán expresarse de manera clara e inequívoca, garantizar el cumplimiento de los requisitos establecidos en la LSSICE y en las normas de ordenación del comercio y facilitar el enlace a las condiciones de acceso y, en su caso, de participación; todo ello sin perjuicio de cuanto dispongan las normas dictadas por las Comunidades Autónomas con competencias exclusivas en materia de consumo. Por último, queda prohibido este envío en aquellos supuestos en los que se disimule u oculte la identidad del iniciador o remitente por cuenta de quien se efectúa la comunicación comercial (supuesto del intermediario) o que inciten a los DSSI a visitar páginas de Internet que contravengan lo dispuesto en este precepto.

Más controvertido es el artículo 21 LSSICE, que, como veremos, parte del artículo 7 DCE para optar por un enfoque radicalmente distinto. Este precepto contempla una prohibición taxativa del envío de comunicaciones comerciales, publicitarias o promocionales, por correo electrónico u otro medio equivalente, «que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas»[277]. Como podemos observar, a diferencia de la política legislativa defendida por la DCE, la norma española se inclina por un sistema *opt-in*, estableciendo la licitud de la comunicación comercial únicamente si, con carácter previo, el DSSI o receptor ha solicitado su envío o prestado expresamente su consentimiento, no bastando su mera no oposición (como sucede con el modelo *opt-out*). Constituye una excepción a esta regla general la contenida en el apartado segundo del mismo artículo 21 LSSICE, en virtud del cual el envío de publicidad a través de la Red resultará legal cuando exista una relación contractual previa entre el emisor (PSSI) y el receptor (DSSI) del mensaje, siempre que aquel hubiera obtenido los datos de contacto del DSSI de manera lícita

veracidad publicitaria y la prohibición de publicidad engañosa». Sobre esta cuestión, de manera tanto más profusa, *vid.* URÍA MENÉNDEZ, R., *Derecho mercantil*, Madrid, Marcial Pons, 1999, p. 93.

[277] Como bien apuntara ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., p. 244, esta definición «resulta cuanto menos incompleta, puesto que lo que caracteriza al *spam* precisamente no es su soporte electrónico, sino la difusión masiva del mensaje publicitario en una dimensión tan sólo alcanzable –y probablemente rentable– en un soporte de dicha naturaleza: esa masificación del mensaje de datos resulta no obstante olvidada por la legislación española que de tal manera somete a la misma regla la gran emisión de millones de mensajes de datos de contenido publicitario con la emisión de un mensaje de datos de idéntico contenido llevada a cabo en forma aislada o semiaislada y casi *inuitu personae* como igualmente suele acontecer en el ámbito electrónico».

y los emplee tan sólo a los efectos de envío de comunicaciones comerciales relativas a productos o servicios de su propia empresa que sean similares a aquellos que, en su momento, fueron objeto de contratación con el cliente[278]. En todo caso, el PSSI tendrá la obligación de ofrecer al DSSI la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de la recogida de los datos como en cada una de las comunicaciones comerciales que le dirija. Además, cuando hubieran sido remitidas por *e-mail*, en él se deberá incluir necesariamente una dirección de correo electrónico u otra dirección electrónica válida donde pueda ejercitarse este derecho, quedando prohibido el envío de comunicaciones comerciales que no incluyan esta dirección[279].

Aun siendo legal el envío de comunicaciones comerciales, el artículo 22 LSSICE da la posibilidad al DSSI, con una simple notificación al PSSI, de revocar en cualquier momento posterior el consentimiento prestado para la recepción de mensajes publicitarios o promocionales. Para ello, será necesario que el remitente habilite (y facilite información accesible) procedimientos sencillos y sin coste alguno, siendo suficiente, de haberse practicado vía correo electrónico, la inclusión de una dirección de correo electrónico u otra dirección electrónica válida donde poder ejercitar este derecho, quedando prohibido el envío de comunicaciones que no incluyan dicha dirección. A efectos comerciales, la LSSICE brinda a los PSSI la posibilidad de utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los DSSI (*cookies*), exigiéndose, también aquí, el previo consentimiento (que, siempre que sea técnicamente posible y eficaz, podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones) tras haber recibido información

[278] De este modo, el artículo 21.2.1º LSSICE tiende a corregir, atenuándolo (en escasa medida), el rigurosísimo régimen prohibitivo y sancionador del *spam* establecido en la redacción original de la norma. Ello ha tenido también un acertado reflejo en la interpretación judicial que de dicho precepto se ha producido a partir de ese momento, que ha tendido a una postura más favorable a la legalidad de la publicidad electrónica. Así, como ejemplo, se ha declarado la licitud del envío de comunicaciones comerciales no solicitadas a quien entregó al iniciador una tarjeta de visita con una dirección de correo electrónico en una feria de muestras en la que, ni siquiera, había adquirido producto alguno del anunciante o de sus agentes (SAN de 17 de mayo de 2007, F. J. 3º).

[279] CAMPILLOS GONZÁLEZ, G. M., «La Ley de servicios de la sociedad de la información: marco jurídico de las actividades económicas a través de Internet», *Economía industrial*, vol. 338, 2001, pp. 55 y 56; MADRID PARRA, A., «Contratación electrónica y protección de datos personales», *Revista de la contratación electrónica*, vol. 94, 2008, pp. 3 y 4.

clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto por la LOPDCP, habida cuenta de que, de su empleo, pueden desvelarse aspectos comprensivos de la esfera privada de los usuarios. Esto no impedirá, no obstante, el posible almacenamiento o acceso técnico a los solos efectos de realizar la transmisión por una red de comunicaciones electrónicas o, en la medida en que resulte estrictamente necesario, para la prestación de un SSI solicitado de manera expresa por el DSSI[280].

[280] Definidas por DI COCCO, C. Y OTROS, *Temi di Diritto dell'informatica*, cit., p. 5, las *cookies* son registros de datos relativos a nuestras interacciones con los sitios de Internet. El 7 de junio de 2012, el Grupo de Protección de Datos del artículo 29 DPPFTDP elaboró el Dictamen 4/2012 (00879/12/ES WP 194), en el que se indican cuáles son las *cookies* que se hallan exentos del deber de solicitar el consentimiento del DSSI de una manera informada, siempre que no se utilicen para otros fines adicionales. Estas *cookies* son las siguientes: en primer lugar, las *cookies de entrada del usuario*, que son aquellas *cookies* de sesión que se utilizan para rastrear las acciones del usuario en una serie de intercambios de mensajes con un PSSI de manera coherente, de modo que serían *cookies* de origen, normalmente asociadas a un identificador de sesión, que expiran, a más tardar, al terminar la sesión; en segundo lugar, las *cookies de autenticación*, que se utilizan para identificar al usuario desde el momento en que inicia la sesión, siendo necesarias para que los usuarios puedan autenticarse por sí mismos en sus visitas sucesivas al sitio web y acceder al contenido autorizado; en tercer lugar, las *cookies de seguridad del usuario*, que son introducidas específicamente para reforzar la seguridad del servicio solicitado explícitamente por él, como es el caso, por ejemplo, de las *cookies* utilizadas para detectar intentos erróneos y reiterados de conexión a un sitio web o de otros mecanismos similares para proteger el sistema de conexión frente a los abusos; en cuarto lugar, las *cookies de sesión de reproductor multimedia*, también conocidas como *flash cookies*, que se utilizan para almacenar los datos técnicos necesarios para reproducir contenidos de vídeo o de audio, como la calidad de la imagen, la velocidad de conexión a la Red o los parámetros de almacenamiento temporal; en quinto lugar, las *cookies de sesión para equilibrar la carga*, que son *cookies* que permiten distribuir el tratamiento de las solicitudes de un servidor web entre un conjunto de máquinas de reserva en lugar de una sola; en sexto lugar, las *cookies de personalización de la interfaz de usuario*, que se emplean para almacenar una preferencia del usuario en relación con un servicio en las páginas web y que no están vinculadas a otros identificadores persistentes, como el nombre del usuario, y, en séptimo y último lugar, las *cookies de complemento (plug-in) para intercambiar contenidos sociales por miembros conectados a una red social*. Por su parte, las *cookies* no exentas del deber de solicitar consentimiento por parte del DSSI de una manera informada, de acuerdo con lo establecido en el artículo 22.2 LSSICE, serían los siguientes: en primer lugar, las *cookies de complemento (plug-in) de contenidos sociales para el seguimiento*, que son utilizadas para realizar el seguimiento de personas; en segundo lugar, las *cookies de terceros*, que se emplean en la publicidad comportamental, y, en tercer lugar, las *cookies empleadas para realizar análisis por los propietarios de sitios web*, a fin de estimar el número de visitantes especiales, detectar las principales palabras clave de los motores de búsqueda que conducen a una página web o rastrear aspectos de la navegación en el sitio web. Este Grupo de Trabajo se creó con arreglo al artículo 29 de la precitada Directiva, ya derogada, siendo sus tareas descritas en el artículo precedente

## III. OPERACIONES ESTRICTAMENTE NEGOCIALES: LA CONTRATACIÓN ELECTRÓNICA

Esta actividad previa de carácter publicitario o promocional en que consiste el envío de comunicaciones comerciales virtuales puede (y suele) desembocar, como decíamos, en la celebración de *contratos electrónicos* o *contratos celebrados por vía electrónica*, categoría que ocupa un lugar principal en el presente estudio y que, por ende, pasamos a analizar.

### 1. Concepto

El contrato celebrado por vía electrónica se encuentra definido en el apartado h) del anexo LSSICE (la DCE no proporciona definición alguna al respecto) como todo contrato en que tanto la oferta como la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos (cable, radio, medios ópticos o cualquier otro de naturaleza electromagnética) que se hallen conectados a una red de telecomunicaciones[281]. Comprenderá, pues, todos aquellos contratos que sean celebrados a través del intercambio de

y en el artículo 15 DPCE. Con la entrada en vigor del RPPFTDP, se planteó la necesidad de que el Comité Europeo de Protección de Datos sustituyera a dicho Grupo, dictándose un artículo 94 en el que, además de la derogación de la DPPFTDP con efectos a partir del próximo 25 de mayo de 2018 (apartado primero), se dispone que «[t]oda referencia al Grupo de protección de las personas en lo que respecta al tratamiento de datos personales establecido por el artículo 29 de la Directiva 95/46/CE se entenderá hecha al Comité Europeo de Protección de Datos establecido por el presente Reglamento» (apartado segundo). En nuestro país, la AEPD también ha procedido a publicar, con fecha de 29 de abril de 2013, una *Guía sobre el uso de las cookies*, que recoge las orientaciones, garantías y obligaciones que la industria se compromete a difundir y aplicar para adaptar este tipo de archivos a la legislación vigente.

[281] En el Anteproyecto de Ley de 21 de enero de 2001, el contrato celebrado por vía electrónica era definido como «todo contrato celebrado sin la presencia física simultánea de las partes, prestando estas su consentimiento en origen y en destino por medio de equipos electrónicos de tratamiento y almacenaje de datos, conectados por medio de cable, radio, medios ópticos o cualquier otro medio electromagnético». En la redacción actual desparece la referencia a la ausencia de presencia física simultánea de las partes, entiendo que por razones de obviedad, habida cuenta de que estamos, de un lado, ante una modalidad concreta de SSI, donde una de sus características esenciales es que sea prestado a distancia y, de otro, ante una vertiente de contratación a distancia. También se sustituye la alusión a la necesidad de que el consentimiento esté prestado en origen y en destino por medio de equipos electrónicos de tratamiento y almacenaje de datos por la actual de que la oferta y la aceptación se transmitan por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones. En cualquier caso, conviene destacar, como en su momento hiciera PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», en PLAZA PENADÉS, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, p. 182, cómo con esta definición genérica por la actual LSSICE se deja abierta la puerta a la posibilidad de poder contratar electrónicamente a

mensajes de datos por medios electrónicos[282]. La transmisión inmaterial de las declaraciones negociales y la marginación del papel como material será el elemento característico y la consecuencia inevitable de un cauce de manifestación de voluntades negociales de muy diversa naturaleza que tienen en el empleo de medios electrónicos su punto común o de convergencia.

La Sección 3 del Capítulo II (artículos 9 a 11) DCE regula esta vía contratación, que será el SSI por excelencia (encuadrable, a su vez, en el comercio electrónico) y la más importante y trascendente de las aplicaciones que, en el plano jurídico, posee la electrónica (**anexo III**)[283]. Lo propio hará la LSSICE en su Título IV (artículos 23 a 29).

Como podemos advertir de lo anterior, la oferta *online*, por sí sola, no hace nacer vínculo contractual alguno si la aceptación a dicha oferta no se efectúa a través de un medio de la misma naturaleza; lo mismo sucedería con aquellos supuestos en los que la aceptación emitida no va precedida de una oferta realizada en el mismo contexto virtual. Con ello se pone de manifiesto que la realización de algunos de los trámites que conforman el procedimiento contractual por medio de la electrónica no basta, *per se*, para conferir a los contratos resultantes la naturaleza de la que hablamos, siendo necesario, repetimos, que, al menos, tanto la oferta como la aceptación se plasmen digitalmente.

Ello nos va a llevar a hablar de dos "tipos" de contratación electrónica: en primer lugar, una contratación electrónica en sentido estricto, que es aquella en la que el contrato se perfecciona y concluye a través de redes informáticas (ya que es en este medio donde tiene lugar tanto la oferta como la aceptación contractual), siendo su régimen jurídico el específico de la contratación electrónica, contenido tanto en la normativa de SSI y de comercio electrónico como en el régimen general de la contratación; en segundo lugar, una contratación electrónica en sentido amplio o impropio, que es aquella otra en la que, si bien el contrato no se perfecciona *online* (ya sea por razón de la materia o por la necesidad de completar formalidades

través de cualquier otro instrumento o aparato que, distinto del ordenador, se halle conectado a una red de telecomunicaciones; este sería el supuesto, entre otros, de la contratación electrónica practicada a través de una pantalla de televisión (*t-commerce*) o del teléfono móvil (*m-commerce*).

[282] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 5.

[283] En torno a la distinción entre comercio electrónico y contratación electrónica, *vid.* VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 89 y 90.

*offline*), algunos de los trámites encaminados a la perfección y/o a la conclusión del contrato se realizan por medio de equipos electrónicos, combinándose, por tanto, actuaciones en línea con actuaciones fuera de línea y siendo de aplicación el régimen general de la contratación más la normativa especial de SSI y de comercio electrónico sólo (a diferencia del supuesto anterior) para aquellos trámites realizados de manera virtual[284].

La novedad que supone la aparición de la contratación electrónica no reside en constituir una nueva modalidad de contrato (que no lo es), sino en conformar un nuevo medio a través del cual vehicular o perfeccionar las declaraciones jurídicas de voluntad entre ausentes[285]. Es por esta razón que, pese a utilizarse con frecuencia ambos términos de manera indistinta, entiendo que resulta más adecuado hablar de *contratación celebrada por vía electrónica* que de *contratación electrónica*.

Por lo demás, estos contratos no constituyen una realidad exclusiva de Internet, que es tan sólo uno de los medios de comunicación empleados para su formación, bien es cierto que el principal y más importante en la actualidad (de ahí que, en multitud de ocasiones, los empleemos como sinónimos), pues, pese a que la contratación electrónica nace unida a fenómenos como el EDI, la expansión de la utilización de las redes electrónicas de comunicación para la formación (e, incluso, ejecución) de los contratos está ligada al desarrollo de Internet, que los traslada a un entorno diferente (el de las redes electrónicas abiertas y descentralizadas) y posibilita su uso generalizado para la adquisición de bienes y servicios de todo tipo[286].

La admisibilidad de los contratos celebrados por vía electrónica en nuestro ordenamiento jurídico deriva, con carácter general, del amplio ámbito de autonomía reconocido a los contratantes para formalizar y configurar sus relaciones. En este sentido, cabe señalar, como punto de partida, la aplicación a estos contratos de las disposiciones generales sobre obligaciones contractuales o relativas al tipo contractual de que se trate (típicamente, CC o

[284] PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», cit., pp. 181 y 182.

[285] A favor de esta concepción instrumental del contrato electrónico, *vid.* BOLÁS ALFONSO, J., «Firma electrónica, comercio electrónico y fe pública notarial», *Revista jurídica del notariado*, vol. 36, 2000, p. 31.

[286] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 5 a 8.

CCom[287], además del TRLGDCU [Título I –artículos 59 y ss.–, Título II –artículos 80 y ss.– y Título III –artículos 92 y ss.– del libro segundo], la LOCM[288] (artículo 38) o en la LCGC[289] –aplicables a todos los contratos celebrados mediante CGC, sean o no de consumo–)[290], si bien su funcionamiento en determinados sectores de la actividad económica que son objeto de especiales controles públicos (como ocurre con el mercado de valores) puede estar subordinado al establecimiento de un marco regulador especial.

No obstante, las características propias de este nuevo canal de contratación determinan la inadecuación de las soluciones normativas que, en su día, fueron creadas para dar respuesta

[287] BOE núm. 289, de 16 de octubre de 1885.

[288] BOE núm. 15, de 17 de enero de 1996. Como bien expone GALLEGO PEREIRA, M. D. Y OTROS, *La Web 2.0: una visión empresarial y jurídica*, cit., p. 4, con anterioridad a la redacción del apartado cuarto de la D. F. 2ª LMTRLGDCU (BOE núm. 76, de 28 de marzo de 2014), el artículo 38 LOCM contenía un apartado sexto que rezaba lo siguiente: «cuando la contratación a distancia de bienes o servicios se lleve a cabo a través de medios electrónicos, se aplicará preferentemente la normativa específica sobre servicios de la sociedad de la información y comercio electrónico». Esto fue interpretado de la siguiente manera: en los extremos en que ambas leyes (LSSICE y LOCM) entren en conflicto por regular los mismos asuntos pero de distinto modo, habrá de acogerse la solución legal de la LSSICE; en cambio, en aquellos otros aspectos en que no quepa advertir discrepancias legales, ambas leyes habrán de aplicarse concurrentemente. En todo caso, las disposiciones destinadas a regular las relaciones jurídicas con los consumidores en los contratos a distancia de bienes y servicios contenidas en la LOCM fueron refundidas en el TRLGDCU; resultado de ello, en el apartado segundo de la Exposición de Motivos de esta última norma queda circunscrito el ámbito de aplicación a estos efectos de la LOCM: «[c]omo consecuencia de esta refundición la regulación sobre contratos a distancia contenida en la Ley 7/1996, de 15 de enero, queda vigente para la regulación de las relaciones empresariales». Posteriormente, esa previsión quedó superada con la LMTRLGDCU, que, en el apartado primero de su D. D. Única, suprime los artículos 39 a 48 LOCM, relativos a las ventas a distancia, decisión esta que queda justificada por el ánimo de «evitar la confusión que genera la existencia de un régimen duplicado para los contratos de venta a distancia en esta norma y en la citada Ley, cuyo contenido sobre venta a distancia resulta desfasado» (apartado III de la Exposición de Motivos).

[289] BOE núm. 89, de 14 de abril de 1998. El artículo 5.4 LCGC (inicialmente, artículo 5.3 LCGC), sobre contratación telefónica y electrónica con CGC, y el controvertido RDCGC (BOE núm. 313, de 31 de diciembre de 1999), fueron derogados por mor de la D. D. Única.2 y 3 de la LMTRLGDCU.

[290] Esta normativa, accesoria en lo que ahora nos concierne, conoce y respeta las peculiaridades propias de la contratación electrónica, motivo que justifica la remisión que a la LSSICE hace el artículo 94.1º TRLGDCU, poniendo de manifiesto la prevalencia de aquella respecto a esta (a excepción de lo dispuesto en el artículo 97.7.2º TRLGDCU) en los supuestos de regulación jurídica discordante

a contratos tradicionales expresados en forma oral o escrita. El resultado inmediato no debe sorprender a nadie: la radical novedad del entorno en el que han de concurrir de manera progresiva los intereses de los individuos genera desconfianza en los actores protagonistas del cambio, que dudan de la validez y eficacia de las transacciones virtuales, al tiempo que ocasiona una previsible y esperada lentificación del desarrollo inicial del magno proyecto. Es este incipiente contexto el que impulsa al legislador comunitario (posteriormente, y sobre esta base, al nacional, precedidos ambos de orientaciones a escala mundial –LMCE y LMFE, fundamentalmente–) a despejar dudas y a generar seguridad en esta nueva vía de contratación desmaterializada, con el anhelado fin de promoverla y potenciarla a medio y largo plazo, sea mediante la eliminación de los obstáculos derivados de la existencia de disparidades legislativas[291], sea a través de la adaptación del Derecho preexistente a sus peculiaridades, sea merced a la creación de reglas uniformes sobre la materia.

[291] Los ámbitos relativos a la contratación electrónica, a la contratación a distancia y a la contratación con CGC tienen (y deben seguir teniendo) ámbitos de actuación separados y distintos que justifican su regulación fragmentada, resultante, en gran parte, de la incorporación, también fragmentaria, de la normativa comunitaria. La intervención europea en el ámbito de la contratación electrónica tiene por objetivo fundamental favorecer la armonización o coherencia entre las distintas legislaciones de los Estados miembros, con los beneficios, más que patentes, que ello supone para el mercado interior, pues la expansión de los mecanismos electrónicos multiplica las posibilidades con que cuentan los operadores económicos de comercializar sus bienes y servicios a lo largo y ancho del territorio de la UE. No obstante la idea de coordinación normativa, el limitado alcance que presenta la armonización del Derecho contractual en general hace que elementos clave de la contratación electrónica no hayan sido objeto de regulación en la DCE, orientada, tan sólo, a proporcionar ciertas reglas básicas o estructurales, pero con carencias significativas en aspectos importantes, como la distinción entre ofertas e invitaciones a presentar ofertas, la concreción del momento de perfección del contrato o la respuesta a dónde y cuándo se considera expedida y recibida una comunicación electrónica (salvo la regla puntual del artículo 11 sobre recepción del pedido y acuse de recibo). De ahí que corresponda a cada uno de los Estados miembros la tarea de, partiendo de la normativa comunitaria, regular estos aspectos, como sucede con la LSSICE, que incluye la regulación de ciertos elementos adicionales, como los relativos a la forma y prueba de los contratos celebrados por vía electrónica, la intervención de terceros de confianza o la determinación de la ley aplicable y del lugar de celebración del contrato. A ello se añade la reducción en la capacidad de actuación que a la Directiva impone la existencia de otras previas sobre aspectos relacionados con su ámbito de actuación en materia de contratación electrónica, como es el caso de la DCACCC (DOCE L 95, de 21 de abril de 1993, p. 29), de la DAAEDE (DOUE L 267, de 10 de octubre de 2009, p. 7), de la DDC (DOUE L 304, de 22 de noviembre de 2011, p 64), o, más recientemente, del RIE-SCTE.

## 2. El principio de libertad de forma en la doctrina contractualista

La cuestión de la *forma*, en cuanto elemento natural del contrato, admite una pluralidad de interpretaciones que, como no podía ser de otra manera, genera ciertas dificultades en la concreción de su significado[292]. En su sentido más amplio y general, la forma puede ser definida como la expresión o manifestación sensible de todo fenómeno jurídico, la manera de revelarse su propia existencia[293], el vehículo o medio (sea cual sea) de exteriorización de las declaraciones de voluntad individual que constituyen el motor del negocio jurídico o, en fin, la razón por la cual los actos internos pueden ser conocidos y, en consecuencia, tener relevancia para el mundo del Derecho[294]. Por ello, comoquiera que el contrato debe comunicarse para desprender los efectos que le son propios, podemos afirmar que siempre será formal, pues siempre necesitará de alguna forma para celebrarse y exteriorizarse[295].

Pese a lo anterior, la doctrina viene entendiendo por formalismo, desde un punto de vista ciertamente más restringido o limitado, el cauce concreto empleado para manifestar la voluntad contractual, es decir, «el principio en virtud del cual una determinada formalidad es exigida por la ley para la validez de un acto»[296]. En otras palabras, será formal aquel contrato que requiera de un revestimiento o requisito adicional a la declaración de voluntad que, exigido preceptivamente por la ley o por las partes, sea determinante de la válida constitución de dicho contrato[297].

Al respecto, los fines perseguidos con la forma pueden ser varios (**anexo XII**): en unos casos, se buscará la publicidad del contrato y la consiguiente eficacia respecto de terceros, como sería el supuesto de la escritura e inscripción registral de la hipoteca (artículo 1875 CC); en otros, se perseguirá otorgar al contrato una posición relevante en detrimento de otros,

---

[292] DE CASTRO Y BRAVO, F., *El negocio jurídico*, Madrid, Civitas, 1967, p. 277.

[293] PUIG BRUTAU, J., *Fundamentos de Derecho civil*, Vallirana, Bosch, 1979, p. 148.

[294] VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., p. 127.

[295] *Ibid.*, p. 127.

[296] GUILLIEN, R./VINCENT, J., *Lexique de termes juridiques*, París, Dalloz, 1990, p. 242.

[297] TOSI, E., *Il contratto virtuale*, cit., p. 264.

como sucede con los relativos a los créditos privilegiados (artículos 90 y ss. LC[298]); en algunas ocasiones, tratará de generar una mayor vinculación (de carácter psicológico) en los contratantes[299]; otras veces, en cambio, tendrá por objetivo imprimir determinados efectos a un derecho, como la incorporación de un crédito a un documento para permitir su circulación, si bien, en definitiva, lo normal será que pretenda asegurar la preconstitución de la prueba del contrato, conocida como *función de certidumbre*, que permitirá determinar concretamente los elementos y el contenido del contrato y que podrá tener lugar en sentido positivo (cuando queda establecida una manera concreta de aportar la prueba –necesidad de documento escrito, aunque, como vimos, también entendemos incluido el que consta en forma visual o sonora–) o en sentido negativo (cuando, entre otros supuestos, para la prueba de alguna declaración contractual no basta la declaración de testigos)[300].

Resultado de lo anterior, podemos diferenciar, al modo clásico o tradicional, una forma *ad solemnitatem*, necesaria para la validez del acto, y una forma *ad probationem*, encaminada a la prueba del contrato. No obstante, en la actualidad, dadas las notas definitorias que adquiere nuestro sistema jurídico, están apareciendo nuevos criterios, complementarios, a la hora de clasificar la forma, de tal modo que también se habla de forma *informativa*, cuyo fin es el de proteger a la contraparte en los supuestos de contratación asimétrica, o de una forma *ad regularitatem*, que contemplará fines (como los publicitarios o los fiscales) distintos a la validez del acto[301]. A la vista de todo lo anterior, la cuestión principal residirá en discernir si el medio electrónico permite satisfacer, o no, los requisitos formales de validez, prueba, información o regulación del negocio jurídico *supra* enumeradas.

---

[298] BOE núm. 164, de 10 de julio de 2003.

[299] VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., pp. 128 y 129.

[300] PUIG BRUTAU, J., *Fundamentos de Derecho civil*, cit., pp. 153 y 154. Sobre los efectos de la forma en el contrato electrónico, *vid.* MORENO NAVARRETE, M. Á., *Derecho-e: Derecho del comercio electrónico*, Madrid, Marcial Pons, 2002, pp. 42 y 43.

[301] Sobre esta cuestión, *vid.* COGLIOLO, P., *Filosofia del Diritto privato*, Florencia, Barbera, 1891, p. 230.

## 3. El problema del formalismo indirecto

La doctrina mayoritaria, en línea con nuestro sistema jurídico actual, proclama el *principio general espiritualista o de libertad de forma de los contratos*[302], también conocido como *principio consensualista*[303], en virtud del cual, el contrato será válido con independencia del medio empleado para su exteriorización[304]. Así, lo verdaderamente importante para poder hablar de un contrato electrónico válido y eficaz no es la forma, sino el aspecto consensual o espiritual, de tal modo que, desde que hay consentimiento, existe contrato, independientemente del registro y el soporte físico que hayan sido empleados por las partes para manifestarlo[305]. A partir de

[302] Sobre el principio espiritualista o de libertad de forma y su aplicación a la contratación electrónica, *vid.* MIRANDA SERRANO, L. M. Y OTROS, *La contratación mercantil. Disposiciones generales. Protección de los consumidores*, cit., pp. 1 y ss.; PERALES VISCASILLAS, P., «Forma del contrato», en BOTANA GARCÍA, G. A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, Wolters Kluwer, 2001, pp. 370 y 371; RICO CARRILLO, M., «La forma en la contratación electrónica», *Derecho de los negocios*, vol. 172, 2005, pp. 1 y ss.

[303] MAS, F., *La conclusion des contrats du commerce électronique*, París, Lgdj, 2005, p. 207.

[304] En esta línea se encuentran autores como BETTI, E., *Teoria generale del negozio giuridico*, Turín, Utet Giuridica, 1952, pp. 285 y ss.; DAHM, W., *Deutsches recht*, Stuttgart, Kohlhammer, 1951, pp. 12 y ss.; DE LOS MOZOS Y DE LOS MOZOS, J. L., «La forma del negocio jurídico», *Anuario de Derecho civil*, vol. 4, 1968, pp. 70 y ss.; FERRI, G. B., «Forma e autonomia negoziale», *Quadrimestre*, vol. 1, 1987, pp. 313 y ss.; GENOVESE, A., *Le forme volontarie nella teoria dei contratti*, Padua, Cedam, 1949, pp. 282 y ss.; HOLMES, O. W., *The common law*, Boston, Little Brown, 1923, pp. 270 y ss.; IHERING, R. V., *Geist des römischen rechts auf den verschiedenen stufen seiner entwicklung*, Leipzig, Breitkopf und Härtel, 1865, pp. 490 y ss.; ROPPO, V., *Il contratto*, Bolonia, Il Mulino, 1977, pp. 88 y ss.; SANTORO PASSARELLI, F., *Dottrine generali del Diritto civile*, Nápoles, Jovene, 1986, pp. 135 y ss.

[305] No coincido con autores como TOSI, E., «La conclusione dei contratti online», en TOSI, E. (coord.) *I problemi giuridici di Internet*, Milán, Giuffrè, 2003, p. 105, o VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., p. 132, a la hora de entender (en línea con la descripción técnica FERNÁNDEZ DOMINGO, J. I., *Algunas notas acerca de la contratación y el comercio electrónico*, Valencia, Tirant lo Blanch, 2003, p. 255) que de la declaración de voluntad emitida electrónicamente hace que estamos ante una nuevo forma de manifestación del consentimiento, ya que, con la aparición de la contratación electrónica, dicha manifestación sigue produciéndose a través de la voz y de la escritura. Y es que, como tuve ocasión de expresar a la hora de analizar la naturaleza jurídica del documento electrónico, entiendo que la innovación que supone este nuevo canal de exteriorización de la voluntad negocial no consiste en la sustitución de la forma oral o escrita en el contrato (que, como expresiones fundamentales de comunicación entre individuos, seguirán, no sólo existiendo, sino predominando), sino en la aparición de un nuevo soporte físico con el que poder vehicular estas tradicionales formas de comunicación, soporte físico que no sustituye (al menos por el momento) sino que complementa el tradicional en papel.

este instante, las partes quedarán obligadas al cumplimiento de lo pactado y a las consecuencias que, según su naturaleza, sean conformes a la buena fe[306], al uso o a la ley (artículos 1254 y 1278 CC y 51 CCom, el último en lo que sea de aplicación a este ámbito[307])[308]. En consecuencia, ha sido habitual la admisión de la eficacia obligatoria de las declaraciones de voluntad expresadas a través de mensajes de datos con anterioridad, incluso, a la aparición de la normativa regulatoria del contrato electrónico.

No obstante lo anterior, una cosa hay clara, y es que, con las nuevas tecnologías, se impone la obligatoriedad del soporte: mientras que el contrato tradicional podía celebrarse válidamente en forma escrita o hablada (sin necesidad, la primera, de forma especial, y, esta última, de soporte físico), el contrato electrónico, presente la forma que presente, ha de canalizarse, obligatoriamente, de manera electrónica (rasgo definitorio básico de este tipo de contratos). Por tanto, partiendo de la concepción restringida o limitada de la forma contractual, aun no siendo necesaria, *a priori*, su constancia en soporte físico distinto del papel pero apto para el

[306] El artículo 3 LMCE sigue la estela de los artículos 7 y 80 CNUCCIM, donde la buena fe se consagra como principio básico en orden a interpretar y ejecutar contratos de compraventa internacional. Su fundamento se encuentra en la necesidad de confianza para un ámbito, como es el comercio electrónico, donde se manifiesta con fuerza el axioma en virtud del cual la ignorancia de la innovación genera desconfianza. En el ámbito de la contratación electrónica, se trata de una manifestación del principio de inalterabilidad del Derecho preexistente de obligaciones y contratos privados (ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., p. 334); en la misma línea, VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., p. 79, quien sostiene que establecer la buena como uno de los principios básicos de la contratación electrónica significa, «[…] en un sentido, una concreta manifestación del postulado de la inalterabilidad del Derecho preexistente de las obligaciones privadas en el campo de la contratación electrónica y, en otro, un postulado de afirmación rotunda en un medio contractual extremadamente novedoso y de gran complejidad técnica».

[307] En concreto, señala BERCOVITZ RODRÍGUEZ-CANO, A., *Apuntes de Derecho mercantil: Derecho mercantil, Derecho de la competencia y propiedad industrial*, Cizur Menor, Aranzadi, 2011, p. 170, no es aplicable analógicamente a la contratación electrónica lo dispuesto en el apartado segundo del artículo 51 CCom, según el cual «[l]a correspondencia telegráfica sólo producirá obligación entre los contratantes que hayan admitido este medio previamente y en contrato escrito, y siempre que los telegramas reúnan las condiciones o signos convencionales que previamente hayan establecido los contratantes, si así lo hubiesen pactado». Ello no impide, continúa este autor, que las partes, en uso de su autonomía de la voluntad, acuerden aplicar a su correspondencia por vía electrónica un régimen similar al previsto en dicho artículo 51.2 CCom.

[308] MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., pp. 83 y 84.

archivo de información de naturaleza electrónica como presupuesto para la validez del contrato desde la concepción tradicional de esta exigencia (normalmente escritura pública ante fedatario), es evidente que la inobservancia de este requisito determina la inexistencia misma del contrato por ausencia de toda forma, de las electrónicamente posibles, de códigos encriptados o de lenguaje especial. Podemos hablar, pues, de una formalidad, si se quiere, más profunda o estructural que pretendida o legal, necesaria, en cualquier caso, para la validez del acto desde un punto de vista, no tanto ya jurídico, cuanto natural o sustancial. Resultado de lo anterior, el contrato electrónico responde, al mismo tiempo y de manera inseparable, a la doble finalidad de la forma *ad substantiam* y *ad probationem*: la primera, insistimos, por la necesidad del soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica como *materialización necesaria de la inmaterialidad inherente* del negocio jurídico analizado; la segunda, en fin, como medio necesario para la prueba, no ya de su validez (anterior), sino de su vida o existencia. Hablamos, así, de lo que podríamos denominar *formalismo indirecto*[309] o *formalismo necesario de contratos jurídicamente no formales*, como son los electrónicos. De exigirse, adicionalmente, que el revestimiento externo haya de constar en una forma determinada, estaríamos, no sólo ante un formalismo indirecto, necesario y sustancial, sino también ante un formalismo directo, solemne y legal, necesario, esta vez sí, para dotar de validez jurídica al contrato. No obstante, como bien apunta VEGA VEGA[310], el principio de equivalencia funcional que caracteriza el Derecho electrónico no es, por el momento, total ni absoluto, «[…] pues cuando la ley determine la necesidad de que un contrato se colme con una forma especial o *ad solemnitatem*, no será válida la electrónica hasta que los avances tecnológicos y la legalidad vigente vayan equiparando en todos los ámbitos ambas clases de documentos»[311].

[309] PIEDELIEVRE, A., *Les transformations du formalisme dans les obligations civiles*, París, Thése Française, 1959, pp. 71 y 72.

[310] VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., pp. 134 y 135.

[311] Como ejemplos, este autor indica la forma autógrafa para el testamento ológrafo, que, aunque hoy queda excluido de la LSSICE por ser un acto de sucesión, no impide que, con el tiempo, puedan equipararse, con las garantías oportunas, ambas formalidades. También la D. T. 11ª LN (BOE núm. 149, de 29 de mayo de 1862), introducida por el artículo 115.2 SLMFAOS (BOE núm. 313, de 31 de diciembre de 2001), que excluye el instrumento público electrónico a las matrices «[h]asta que los avances tecnológicos hagan posible que la matriz u original del documento notarial se autorice o intervenga y se conserve en soporte electrónico». Bien es cierto,

Un primer paso, fundamental, en este proceso de adaptación al que nos referimos nace con la DCE, que, partiendo del principio de equivalencia funcional, exige a los Estados miembros, de manera específica, que garanticen que «[…] el régimen jurídico aplicable al proceso contractual no entorpezca la utilización real de los contratos por vía electrónica, ni conduzca a privar de efecto y de validez jurídica a este tipo de contratos en razón de su celebración por vía electrónica» (artículo 9.1 DCE)[312]. Pese a lo anterior, y dada la importante conexión que presentan con la soberanía interna de cada territorio, existen determinadas categorías de contratos en los que esta previsión podría (carácter opcional) quedar excluida, no teniendo cabida en el mundo virtual (artículo 9.2 DCE)[313]; así sucede con los siguientes

continúa, que, en los contratos electrónicos, como contratos a distancia que son, se exigen determinados requisitos formales (como lo dispuesto en el artículo 5 LSSICE); así, el artículo 11 LOCM (también su artículo 47), tras consagrar el principio de libertad de forma, viene a exigir la necesidad de documentar ciertos aspectos del contrato, justificativos de garantías o derechos de los compradores. Por último, también en determinados actos jurídicos se exige la firma electrónica para garantizar la autenticidad y seguridad en la perfección del contrato. En todo caso, estos supuestos no plantean cuestiones de forma, sino problemas de documentación del contrato a efectos probatorios, ya que el ordenamiento jurídico, en aras a tutelar los derechos de la parte contratante más débil, exige la documentación del contrato (convencional o electrónico) a fin de que estos sujetos puedan hacer valer mejor sus derechos, no afectando, en ningún caso, a la validez esencial de aquellos.

[312] Por lo demás, el considerando 34 DCE establece la necesidad de analizar qué legislaciones han de proceder a dicho ajuste, habiendo de versar este examen «[…] sobre todas las fases y actos necesarios para realizar el proceso contractual, incluyendo el registro del contrato», si bien tan sólo se podrán suprimir los obstáculos derivados del régimen jurídico, no los relativos a la imposibilidad de utilizar la vía electrónica en determinados casos (considerando 37 DCE). En cualquier caso, todo cuanto aquí se establece no afecta a la posibilidad que tienen los Estados miembros de mantener o establecer regímenes jurídicos, específicos o generales, en materia de contratos que pueden cumplirse vía electrónica, en particular los requisitos en relación con la seguridad de las firmas electrónicas (considerando 35 DCE). A nivel internacional y con carácter previo, el artículo 11 LMCE desarrolla, en materia contractual, lo dispuesto con carácter general en el artículo 5 LMCE, sobre reconocimiento jurídico de los mensajes de datos y consecuente formación y validez de los contratos.

[313] Esto puede provocar ciertos desajustes entre Estados miembros derivados de la adopción de exclusiones distintas y no coincidentes. Dicho de otra manera, habida cuenta del carácter voluntario de la opción contenida en el artículo 9.2 DCE, la no exclusión de una materia del ámbito de la contratación electrónica no significa, necesariamente, que un contrato pueda concluirse válidamente por medio de mensajes de datos, si, por citar un supuesto concreto, se contrata con consumidores de otros países de la UE y la legislación aplicable (en estos supuestos, la del Estado miembro del consumidor) sí ha procedido a esta exclusión; de ser así, únicamente podríamos celebrar un contrato electrónico si ninguno de los países implicados ha excluido la contratación electrónica de la categoría de que se trate.

tipos de contratos: a) contratos de creación o transferencia de derechos en materia inmobiliaria, con la excepción de los derechos de arrendamiento[314]; b) contratos que requieran por ley la intervención de los tribunales, las autoridades públicas o profesionales que ejerzan su función pública[315]; c) contratos de crédito y caución y garantías presentadas por personas que actúan por motivos ajenos a su actividad económica, negocio o profesión[316], y d) contratos en materia de Derecho de familia o de sucesiones[317]. El último apartado de este artículo llama a los Estados miembros a que comuniquen a la Comisión qué categorías de las anteriores son objeto de la exclusión descrita, siendo preceptivo, además, el envío periódico (cada cinco años) de un informe sobre la aplicación del artículo 9.2 DCE, «[…] explicando los motivos

[314] Como señala GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, cit., p. 239, el motivo de esta posible exclusión no es otro que «[…] el plus de seguridad jurídica requerido en asuntos inmobiliarios, favorecido por la celebración personal de este tipo de contratos, adicionalmente reforzados con la intervención de fedatarios públicos (como notarios o registradores de la propiedad inmobiliaria)». Queda, empero, excluido el de arrendamiento de inmuebles, «[…] dada su mayor flexibilidad que los de compraventa (por sólo citar los más relevantes), lógicamente derivada de la posesión no dominical que aquél implica, lo que lo acomoda muy adecuadamente al tráfico económico y, con ello, a que su celebración electrónica resulte del todo razonable».

[315] Uno de esos casos sería, por ejemplo, el mencionado de la compraventa de bienes inmuebles, si bien el precepto alude también a modalidades bien diferentes: entre los supuestos de necesaria intervención de un tribunal, aquellos relativos a contratos de enajenación de bienes mobiliarios (como las acciones de una sociedad) por parte de una persona incapacitada; entre los casos de preceptiva participación de una autoridad pública, la posible construcción de una autopista, que podría precisar de la intervención del propio gobierno de un Estado, o, como eventual supuesto de actuación de un profesional que ejerza una función pública, la del registrador mercantil ante la fusión entre dos sociedades de esa misma naturaleza (*Ibid.*, p. 239).

[316] El plus de seguridad jurídica exigido para este tipo de operaciones es el que justificaría la posible inadecuación de su celebración por vía electrónica (*Ibid.*, p. 239).

[317] De nuevo, acierta este autor al encontrar la razón de la exclusión, esta vez en los siguientes términos: «[…] es obvio que la vía electrónica no se ajusta en manera alguna a la creación de una institución familiar como el matrimonio, cuyas dimensiones rebasan infinitamente las estrictamente contractuales (siendo evidentemente además precisa para su celebración, la intervención de una autoridad pública o asimilada a ella en sus efectos, como es la eclesiástica en algunos Estados europeos). Tampoco, obviamente, a la redacción de un testamento: no sólo porque de ordinario es también necesaria la intervención de un fedatario público, como es un notario, sino sobre todo porque, igualmente en este supuesto, el componente personal y familiar del negocio jurídico testamentario tiene en él una trascendencia inconmensurablemente mayor que el sólo económico o comercial» (*Ibid.*, pp. 239 y 240).

por los que consideran necesario mantener las categorías a que hace referencia la letra b) del apartado 2, a las que no aplicará el apartado 1» (artículo 9.3 DCE)[318].

Por su parte, la LSSICE (artículos 23 a 29), más allá de las consideraciones precedentes, acoge y proclama de modo expreso (Exposición de Motivos, apartado IV, párrafo 1º) el principio espiritualista o de libertad de forma, en virtud del cual, como hemos visto, lo verdaderamente relevante para poder hablar de un contrato válido y eficaz no es la forma, sino el aspecto consensual o espiritual. Así, partiendo de estas previsiones, dicta el artículo 23, que, en la línea marcada por la DCE, reitera el principio del equivalente funcional al disponer que los contratos electrónicos producirán cuantos efectos estén previstos en el ordenamiento jurídico, siempre que concurran los requisitos necesarios para su validez (artículo 1261 CC): consentimiento (artículos 1262 a 1270 CC), objeto (artículos 1271 a 1273 CC) y causa (artículos 1274 a 1277 CC). También será de aplicación cuanto disponga el CCom y las restantes normas civiles o mercantiles relativas a contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

Como sabemos, la perfección contractual consiste en un acuerdo de voluntades sobre lo que deba ser el objeto y la causa del contrato, de modo que, hasta que no se produzca dicho consentimiento, no hay contrato, sino proceso de formación del contrato, proceso que, si bien en ocasiones puede resultar especialmente complejo, constituyendo una sucesión de ofertas y contraofertas, en otras, en cambio, puede ser extremadamente simple, bastando un mero intercambio de palabras o, incluso, un cruce de gestos, para evidenciar el acuerdo perfeccionador[319]. Este concurso de voluntades en que consiste el consentimiento servirá también para delinear con precisión la mayor o menor complejidad del contenido mismo del contrato, es decir, de sus distintas cláusulas, términos y condiciones, particulares (de ardua discusión) y generales (de mera aceptación)[320].

---

[318] Desconozco el motivo por el que la DCE exige una justificación de los motivos por los que el Estado miembro en cuestión considera necesario mantener las categorías a que hace referencia el artículo 9.2.b) DCE y no ha de proceder de la misma manera respecto de los restantes apartados a), c) y d).

[319] ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 247, 248 y 273.

[320] No es momento ahora de profundizar sobre la interesante cuestión de las condiciones incorporadas a los contratos, tan, por otro lado, minuciosamente estudiadas desde un principio por autores como ALFARO ÁGUILA-REAL, J./PAZ-ARES RODRÍGUEZ, J. C., *Las condiciones generales de la contratación: estudio de las disposiciones*

Especialmente relevante resulta, en materia de consentimiento, la concreción del momento en que, conforme a Derecho, se entiende producido el acuerdo de voluntades. La modificación introducida por la D. A. 4ª LSSICE modifica, dando idéntica redacción, los artículos 1262 CC y 54 CCom, poniendo fin a una situación de disparidad de soluciones que carecía de cualquier justificación[321]. La perfección del contrato, que se produce, como sabemos, por el mero consentimiento (artículo 1258 CC), requiere determinar en qué momento este se entiende producido, es decir, cuándo se considera que ha tenido lugar el concurso de la oferta y de su aceptación sobre la cosa y la causa que han de constituir el contrato (artículo 1262.1º CC). En la contratación entre presentes no suele haber dificultad a la hora de determinar este momento, a diferencia de lo que sucede en la contratación entre ausentes, donde, a lo largo del tiempo, se han ido configurando una serie de soluciones que, con diferentes perspectivas, tratan de concretar este instante y que serán decisivas a la hora de distribuir entre los contratantes el riesgo de pérdida, retraso o alteración de la comunicación en el proceso de transmisión[322] (**anexo XIII**):

Una primera visión se produce de la mano de la *teoría de la cognición*, que sostiene que la aceptación de la oferta sólo producirá los efectos que le son propios a partir del momento en el que el oferente la haya conocido. El CC optó por esta propuesta en su artículo 1262.2, *ab initio*, cuya redacción original disponía lo siguiente: «[l]a aceptación hecha por carta no obliga al que hizo la oferta, sino desde que llegó a su conocimiento». Como fácilmente podemos deducir, que se haga depender la celebración del contrato de la efectiva recuperación del mensaje de datos por el PSSI facilita que la conducta poco diligente de quien realiza la oferta (por ejemplo, desatendiendo su buzón de correo electrónico) pueda obstaculizar dicha

*generales*, Madrid, Civitas, 1991, pp. 1 y ss. o PAGADOR LÓPEZ, J., *Condiciones generales y cláusulas contractuales predispuestas: la Ley de condiciones generales de la contratación de 1998*, Madrid, Marcial Pons, 1999, pp. 1 y ss.

321 MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., p. 85.

322 En línea con cuanto se indica a continuación, *vid.* DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., pp. 218 y 219; DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 64 a 71; MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., pp. 85 y 86; PEGUERA POCH, M. Y OTROS, «Marco jurídico de los servicios de la sociedad de la información y del comercio electrónico», cit., pp. 366 a 369; PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., p. 89; PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», cit., pp. 194 a 197.

celebración y, con ello, perjudicar a un DSSI que, en todo momento, actuó de buena fe enviando su aceptación o conformidad.

Una segunda es la conocida como *teoría de la recepción*, que, por el contrario, afirma la no necesidad de que el oferente haya conocido, de manera efectiva, la aceptación contractual de la contraparte. En este caso, basta simplemente con que la haya podido conocer, es decir, que haya llegado a su esfera de control.

En tercer lugar, se encuentra la *teoría de la expedición o emisión*, que entiende que no es suficiente que el aceptante haya exteriorizado la aceptación, sino que es necesario haberla enviado (por el medio que sea) a la otra parte, es decir, que la aceptación haya salido de su esfera de control. El CCom, en la redacción original de su artículo 54, se inclinó a favor de esta postura: «[l]os contratos que se celebren por correspondencia quedarán perfeccionados desde que se conteste aceptando la propuesta o las condiciones con que ésta fuere modificada».

En último lugar, y como extremo opuesto a la teoría de la cognición, está la *teoría de la declaración o manifestación*. En ella se exige, únicamente, que el destinatario de la oferta haya manifestado la voluntad de aceptarla, no siendo necesario, a diferencia de la concepción anterior, haberla enviado.

Pues bien, como decíamos en un principio, tras la promulgación de la LSSICE (D. A. 4ª)[323] se ha producido la fusión de los dos sistemas, el civil (artículo 1262 CC) y el comercial (artículo 54 CCom), desapareciendo la disparidad de criterios existente hasta entonces entre ambos preceptos[324]. Así, se establece, tanto para los contratos civiles como para los contratos mercantiles, un criterio común, relativo a los contratos a distancia, primero, y a los contratos electrónicos en general, después, y un criterio especial, para los contratos electrónicos celebrados mediante dispositivos automáticos[325].

---

[323] La DCE no regula el momento de formación del contrato.

[324] Esta fusión de criterios entre ambos preceptos, en opinión de algunos autores, hace innecesaria la existencia del artículo 54 CCom por pérdida de su especialidad (PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., p. 89; PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», cit., p. 195).

[325] En todo caso, como bien apunta DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 65, «[…] en este contexto y ante la incertidumbre derivada de la aplicación de alguno de esos criterios al entorno electrónico,

El primero de ellos, aplicable a los contratos a distancia en general, establece que «[h]allándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación (*teoría de la cognición*) o desde que, habiéndosela remitido el aceptante, no puede ignorarla sin faltar a la buena fe (*teoría de la recepción*)»[326]. De este modo, acoge la teoría de la recepción, añadiendo que, de conocer la aceptación (teoría de la cognición), con más razón deberemos tener el contrato por perfeccionado.

Por su parte, el segundo, concerniente a los contratos electrónicos celebrados mediante el intercambio de mensajes de correo electrónico o similares[327], se recoge en el artículo 28.2 LSSICE, que ofrece un criterio para determinar el momento de la recepción (*teoría de la recepción*): cuando la parte a la que vaya dirigida la aceptación pueda tener constancia de ello. Ahora bien, no se contiene en la norma criterio alguno que permita saber qué se entiende por *tener constancia* de la aceptación; para ello, quizás sea posible aplicar por analogía el criterio que sí proporciona la LSSICE en cuanto a la constancia de la recepción de la aceptación mediante acuse de recibo en el apartado segundo de dicho artículo 28.2, donde se establece que «[s]e presumirá que su destinatario puede tener la referida constancia desde que aquél haya sido

una primera vía para superar la falta de seguridad en este ámbito viene constituida por el pacto entre los contratantes acerca del momento de celebración del contrato. La existencia de un pacto de ese tipo es especialmente frecuente en sistemas cerrados y en contratos formalizados mediante el EDI (el artículo 3.3 del Modelo europeo de Acuerdo de EDI recoge una cláusula en este sentido, que opta por la teoría de la recepción, al considerar celebrado el contrato "en el lugar y momento en que el mensaje de EDI que contenga la aceptación de una oferta llegue al sistema informático del oferente"). También puede suceder que el acuerdo sobre el particular se desprenda de los hábitos que las partes tengan establecidos entre sí».

[326] Las cursivas y los paréntesis son nuestros.

[327] En estos casos, prevalece la consideración de que se trata de un medio que hace posible la formación sucesiva (no instantánea) de contratos a distancia en modo electrónico, dado que, por sus características, no es un medio interactivo y no permite el intercambio simultáneo de información ni la comprobación inmediata de las declaraciones de voluntad en sus propios términos; antes al contrario, los mensajes circulan divididos en paquetes por múltiples operadores intermedios hasta llegar a su destino final, donde típicamente se almacenan en un buzón de correo del servidor hasta que el destinatario decide acceder (*Ibid.*, p. 66). Ello, entre otras cosas, concede un mayor *tempus deliberandi* para la prestación del consentimiento entre las partes intervinientes (ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., p. 250). A favor de esta postura la STS núm. 673/1996, de 30 de julio, F. J. 1º, cuando afirma que «[…] el telégrafo, télex, telefax y correo electrónico en todas sus variedades sirven para exteriorizar declaraciones de voluntad que, si bien son comunicativas, no son instantáneas y coincidentes en las conjunciones de voluntad de los contratantes interesados».

almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones». De ser así, y en línea con lo dispuesto por la *teoría de la recepción*, será suficiente que la aceptación del DSSI haya llegado al sitio necesario para que el PSSI pueda acceder a su contenido, evitando que la perfección del contrato quede al arbitrio de quien, pudiendo conocer la aceptación de la oferta negocial, no llega, sin embargo, a hacerlo por negligencia o falta de la diligencia necesaria[328]. Dentro de estos últimos, se establece un criterio especial, referido tan sólo a aquellos contratos celebrados mediante dispositivos automáticos[329].

Y es que, en línea con aquello que, en su momento, expusieran MIRANDA SERRANO y PAGADOR LÓPEZ[330]:

> «[…] aunque no falta quien piensa que de este modo queda aludida la contratación electrónica en su totalidad, parece más razonable entender que esta regla especial es aplicable a los contratos celebrados electrónicamente y en los que no llega a producirse un auténtico diálogo negocial entre las partes contratantes por la razón de que ese diálogo tiene lugar entre el cliente-aceptante y la máquina oferente a través de una página web en la que se indican al aceptante (mediante iconos:

[328] ILLESCAS ORTIZ, R., «La Ley 22/2007 sobre comercialización a distancia de servicios financieros destinados a los consumidores y la dogmática contractual electrónica», *Derecho de la contratación electrónica*, vol. 84, 2007, p. 14.

[329] Cuando, a diferencia del supuesto anterior, la formación del contrato se produce mediante el empleo de servicios interactivos que hacen posible el intercambio simultáneo de información (es el caso de las páginas web), se entiende mayoritariamente que estamos ante medios de comunicación a distancia que permiten una formación instantánea y no sucesiva del contrato, de tal forma que el tratamiento del momento de celebración del contrato ha de ser equiparado al que rige respecto de otros medios instantáneos de similares características, como el teléfono, ya que, en ambos casos, es factible la comprobación inmediata de que la declaración de voluntad ha sido recibida por el destinatario. En estos casos, el hecho de que la conducta concluyente (o, en general, la oferta y la aceptación –si reúne los requisitos precisos para ser considerada como tal–) sea resultado de la actuación automática (sin intervención humana) de un ordenador, no menoscaba de ningún modo su carácter vinculante, al ser la actividad del ordenador resultado de su previa programación, que permite que este responda a las instrucciones recibidas por parte de aquel a cuya voluntad es atribuible la acción automática (DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 66 y 70).

[330] MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., pp. 85 y 89. En contra de esta postura y a favor de su afectación a todo contrato de naturaleza electrónica, *vid.* PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», cit., pp. 195 y 196.

cesta o carro de la compra, etc.) los sucesivos pasos que debe dar, o sea, los llamados contratos electrónicos celebrados mediante simple pulsación de teclas[331]».

Pues bien, en este tipo de contratación electrónica, se considerará que hay consentimiento desde el momento en que se manifieste la aceptación; rige aquí, pues, la *teoría de la expedición*, en la medida en que (pese a parecer a primera vista que nos encontramos ante la teoría de la declaración) se entiende perfeccionado el contrato desde que la aceptante manifiesta su voluntad de celebrarlo, a condición de que esta manifestación se realice por medio de un mecanismo que la recoja automáticamente, lo que implica, no una mera manifestación, sino una verdadera expedición de la aceptación. El problema (al igual que sucede con la teoría de la declaración), se producirá en aquellos supuestos en los que la aceptación no llega al oferente por razones a este no imputables, no pudiendo conocer la aceptación; en estos casos, entiendo, al igual que parte de la doctrina[332], que hubiera resultado más acertado optar por la solución que ya se contenía en el artículo 32 del Anteproyecto de LSSICE de 30 de abril de 2001, que establecía que este tipo de contrato electrónico se entenderá celebrado desde el momento en el que la aceptación del DSSI o la formulación de su petición llegase al sistema de información[333] empleado por el PSSI, de forma que quede en él almacenado y accesible por este último (teoría de la recepción), eliminando, además, todo tipo de diferenciación entre contratos a distancia, contratos electrónicos y contratos electrónicos mediante simple pulsación de teclas[334].

---

[331] La *contratación electrónica automática* o *por máquinas* o *mediante la simple pulsación de teclas*, o, gráficamente, *contratos-click*, continúa, «[…] es una forma de contratación muy habitual en el comercio electrónico, que se caracteriza por que en la página web del proveedor de servicios aparecen iconos o menciones que posibilitan al interesado en adquirir el bien o servicio allí ofertado la celebración del contrato de una manera literalmente automática, mediante la simple acción consistente en pulsar una tecla o clickear con el ratón en el icono o figura que corresponda (con frecuencia, una cesta de la compra), conforme a las instrucciones que aparecen en la propia página web» (MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., p. 87).

[332] PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», cit., pp. 196 y 197.

[333] Por *sistema de información*, de acuerdo con el artículo 2.f) LMCE (explicado en el apartado 102 de la Guía para la incorporación al Derecho interno de la LMCE), «[…] se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos».

[334] Este criterio de la recepción fue, como señala CLEMENTE MEORO, M. E., «Algunas consideraciones sobre la contratación electrónica», *Revista Aranzadi de Derecho patrimonial*, vol. 4, 2000, p. 75, el criterio seguido en los

A nadie escapa la inadecuada estructura seguida por la LSSICE a la hora de determinar la ubicación que han de tener cada una de las especialidades contractuales antes referidas. En efecto, no se entiende por qué no se ha recogido en un mismo precepto (en este caso, en el artículo 1262 CC, plasmado con la misma redacción en el artículo 54 CCom) el momento en el que se ha de entender producido el consentimiento por las partes en los contratos a distancia en general (regulado en los apartados segundo y primero de los artículos 1262 CC y 54 CCom, respectivamente), en los contratos electrónicos sucesivos (actualmente ubicado, si bien de manera un tanto indirecta o interpretativa, en el artículo 28.2 LSSICE) y en los contratos electrónicos automáticos o instantáneos (contenido en los apartados tercero y segundo de los artículos 1262 CC y 54 CC, respectivamente). Todo ello, más allá de que nos inclinemos a favor de una u otra postura, genera una más que justificada confusión, carente de motivación lógica, que fácilmente hubiera podido evitarse infiriendo a la norma una configuración más sencilla en método e inteligible en redacción.

Para poder concretar la aplicación a los contratos electrónicos de reglas como las contenidas en los artículos 1262 CC y 54 CCom, resultan de especial interés (sobre todo en el supuesto de contratos electrónicos celebrados mediante el intercambio de mensajes de correo electrónico o equivalentes) aquellos criterios que permitan determinar tanto el momento de emisión como el momento de recepción de los mensajes de datos. En estos casos, la

---

códigos civiles alemán e italiano, en la Convención de Viena sobre compraventa internacional de mercaderías o en los Principios para los contratos comerciales internacionales en UNIDROIT. Por tanto, y al modo de entender de este autor, hubiera sido más acertado que el criterio de perfección del contrato electrónico mediante simple pulsación de teclas hubiese sido el previsto en la LMCE (artículo 15), que entiende producida dicha perfección desde que la aceptación (emitida electrónicamente) entra en la red de comunicación, escapando ya del control del aceptante y pudiendo ser recepcionada por el oferente, ya que, desde ese momento, tiene la posibilidad de conocer la aceptación, aun cuando, de facto, no lo haga hasta un momento posterior, lo que se ve minimizado por el deber de diligencia de consulta continua de posibles aceptaciones por parte de quienes posibilitan la contratación de sus bienes y servicios a través de la Red y por la obligación de confirmar la recepción de la aceptación (artículo 28 LSSICE).

LMCE (artículo 15), aunque no contiene propiamente normas sobre determinación del momento de celebración del contrato, sí que recoge tales criterios[335], criterios que, en lo sustancial, aparecen reiterados en el artículo 10 CNUUCECI[336]. Conforme a este precepto, a falta de acuerdo en contrario entre emisor y destinatario, se entenderá que el momento de expedición de un mensaje de datos será el de su entrada en un sistema de información que no esté bajo el control del emisor o de su intermediario. Por su parte, el momento de recepción del mensaje, si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, será el momento en que ingrese en este, salvo que el mensaje se envíe a un sistema de información distinto del designado por el destinatario, en cuyo caso se considerará que el momento de recepción será aquel en el que el destinatario recupere dicho mensaje. Si el destinatario no ha designado un sistema de información, la recepción se considerará que tiene lugar cuando el mensaje de datos ingrese en un sistema de información del destinatario[337].

Por lo demás, para celebrar válidamente un contrato electrónico bastará con emitir una declaración negocial vinculante por medio de equipos electrónicos de tratamiento y almacenamiento de datos conectados a una red de telecomunicaciones. No será necesario, pues (aunque, en ciertos casos, puede llegar a ser habitual –caso del EDI–), haber cruzado comunicación previa alguna con la contraparte para acordar la utilización de medios de naturaleza electrónica a los efectos negociales pertinentes (artículo 23.2 LSSICE).

El apartado 4 del artículo 23 LSSICE concluye el precepto estableciendo qué materias quedarán excluidas de su posible celebración por vía electrónica. Así, partiendo de la previsión contenida en el artículo 9.2 DCE, la norma española acoge únicamente la exclusión prevista en el apartado d) de la Directiva, estableciendo que no será de aplicación lo dispuesto

[335] En efecto, no se regula en la LMCE el momento de perfección del contrato electrónico. No obstante, a la vista de las discrepancias existentes entre los diversos sistemas jurídicos, la norma se limita a determinar el momento de envío y recepción de un mensaje de datos, sin pronunciarse respecto de si el contrato se perfecciona en uno u otro de ambos momentos. Sobre esta cuestión, *vid.* ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., pp. 355 y 356.

[336] A/RES/60/21.

[337] Para una explicación más detallada de este artículo, *vid.* puntos 100 a 107 de la Guía para la incorporación al Derecho interno de la LMCE.

en materia de contratación por vía electrónica al Derecho de familia y de sucesiones, añadiendo, en relación con apartado b) de dicha Directiva, que:

> «Los contratos, negocios o actos jurídicos en los que la Ley determine para su validez o para la producción de determinados efectos la forma documental pública, o que requieran por Ley la intervención de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se regirán por su legislación específica»[338].

4. Lugar de celebración del contrato electrónico

Siguiendo la distinción, ya criticada en términos de estructura, marcada por la LSSICE, optamos, sin embargo, en un intento por dotar de una cierta coherencia sistemática a nuestro estudio, por seguir con esta misma diferenciación para responder a la importante cuestión del lugar en que se entienden celebrados los negocios jurídicos de naturaleza electrónica. Esta cuestión, de índole más bien procesal, traerá importantes consecuencias, sobre todo a la hora de determinar el tribunal competente para la resolución de los conflictos surgidos con posterioridad a la celebración del contrato, ya que ciertas normas de Derecho internacional privado emplean este elemento como criterio de conexión en materia de competencia judicial internacional y de ley aplicable.

Así las cosas, por lo que respecta a los contratos entre ausentes no celebrados por vía electrónica, los artículos 1262.2º, *in fine*, CC y 54.1º, *in fine*, CCom establecen que se entenderán celebrados en el lugar en que se hizo la oferta. En cambio, en relación con los contratos electrónicos propiamente dichos, podemos realizar dos consideraciones relevantes:

---

[338] Entre otras, la SLMFAOS, en su Sección 8ª, intitulada *incorporación de técnicas electrónicas, informáticas y telemáticas a la seguridad jurídica preventiva* (artículos 106 a 115), regula el uso de la firma electrónica por parte de notarios y registradores en el ejercicio de sus funciones públicas. El artículo 115.1 SLMFAOS incorpora el artículo 17 bis LN, por el que se contempla la figura del instrumento público electrónico o de las copias electrónicas. La D. T. 11ª LN excluye del instrumento público electrónico, como ya hemos visto, a las matrices, al menos temporalmente. Por su parte, el artículo 96 SLMFAOS modifica la LH (BOE núm. 58, de 27 de febrero de 1946), mientras que el artículo 97 SLMFAOS introduce un cuarto apartado en el artículo 23 CCom para regular la utilización de los medios telemáticos para la información del contenido de los libros de los Registros de la propiedad, mercantiles y de bienes muebles en beneficio de los interesados. En relación con todo ello, *vid.* BONARDELL LENZANO, R., «La seguridad jurídica en las transacciones electrónicas», *Anales de la academia matritense del notariado*, vol. 43, 2005, pp. 142 y 143.

En cuanto a los contratos electrónicos sucesivos o celebrados mediante correo electrónico (artículo 28.2 LSSICE), el artículo 29 LSSICE (sin equivalente en la DCE[339]) efectúa una separación básica entre: a) aquellos en los que ambas partes tengan la consideración de empresario o profesional (B2B), que, salvo pacto en contrario, se considerarán celebrados en el lugar en el que esté establecido el PSSI[340], y b) aquellos otros en que participe un consumidor (B2C), que se presumirán celebrados en el lugar en el que este tenga su residencia habitual. Este apartado, que parte del criterio contenido en el artículo 5 CR[341] (posteriormente, artículo 6 RRI[342], que sustituye al CR en los Estados miembros), merece ser criticado desde el momento en que se configura como una presunción que, por los términos en que está redactada («se presumirán celebrados»), rige únicamente en defecto de pacto entre los contratantes. La

[339] No obstante, algunos instrumentos de carácter general, como la LMCE (artículo 15.4), ofrecen recursos para que, como sucede en España con la LSSICE, los legisladores nacionales adopten decisiones operativas sobre la cuestión, facilitando la elección del lugar de celebración del contrato y haciendo recomendaciones, más o menos expresas, sin llegar, empero, a imponer fórmula específica alguna. En concreto, esta disposición establece que, en defecto de acuerdo entre las partes, se considerará como lugar de expedición el del establecimiento de quien envía el mensaje (en nombre propio o por cuya cuenta actúa un intermediario) y, como lugar de recepción, el lugar del establecimiento del destinatario; no obstante: a) de tener (uno u otro) más de un establecimiento, se tomará en consideración aquel que guarde una relación más estrecha con la operación subyacente y, de no haber operación subyacente, su establecimiento principal; b) si no existe establecimiento, se tendrá en cuenta el lugar de su residencia habitual.

[340] Se adopta, así, el criterio del establecimiento físico, huyendo del alojamiento técnico del sistema de información desde el que opera, dada la inseguridad y dificultad que supondría su determinación (PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», cit., p. 91). Por su parte, DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 72 a 74, establece que esta referencia al establecimiento del PSSI puede ser fuente de confusión, en la medida en que el contrato puede no constar de PSSI y porque puede darse la circunstancia de que ambos contratantes tengan la condición de PSSI en los términos de la LSSICE; yo no estoy de acuerdo con estas matizaciones, ya que, en primer lugar, no se contempla ni en la normativa comunitaria ni en la española el supuesto de contratos electrónicos C2C [este supuesto, como ya hicimos constar anteriormente, no forma parte del ámbito de aplicación de la DCE –considerando 18– ni de la LSSICE –anexo.a).4º.2.º–], y, en segundo lugar, aun cuando, por separado, ambos contratantes tengan la consideración de PSSI en los términos de la LSSICE, dentro de la operación negocial en que consista el concreto contrato electrónico celebrado, una de las partes, obligatoriamente, habrá de actuar con la condición de PSSI y la otra, también forzosamente, con la de DSSI.

[341] DOCE C 27, de 26 de enero de 1998, p. 34.

[342] DOUE L 177, de 4 de julio de 2008, p. 6.

razón estriba en la posición, con frecuencia más débil, que asume el consumidor en la relación negocial, lo que debe obligar al legislador a dotar de una mayor protección a aquellas situaciones en que este intervenga, evitando la indefensión. En consecuencia, hubiera sido adecuado optar por una redacción de corte más imperativo (al modo de «se celebrarán, salvo decisión en contrario del consumidor»), consiguiendo más eficazmente el efecto protector descrito[343].

En cambio, nada dicen los artículos 1262 CC y 54 CCom acerca de dónde se han de entender celebrados aquellos otros contratos, también electrónicos, cuya perfección haya tenido lugar de manera instantánea o inmediata (página web). Así, entiendo que lo más adecuado, dada la generalidad del título en que se enmarca el artículo 29 LSSICE, es considerar que, para ellos, regirán las mismas reglas que las previstas para los contratos electrónicos sucesivos del párrafo anterior. De nuevo, la falta de una estructura normativa adecuada provoca confusiones como las descritas, obligando al jurista a realizar una interpretación extensiva y compleja que, volvemos a incidir, se podría haber evitado con relativa facilidad.

En cualquier caso, no son pocos los autores que subrayan la escasa utilidad con que cuentan estos preceptos para lograr el objetivo perseguido de determinación del lugar de celebración del contrato[344]. La razón estriba en que, si bien en ciertas normas de Derecho internacional privado español el lugar de celebración del negocio es un criterio de conexión relevante (así sucede con los artículos 22 quinquies LOPJ[345] y 10.5 CC, de aplicación residual), su trascendencia práctica es muy limitada, en la medida en que, en materia de ley aplicable, puede verse desplazado por normas de alcance universal recogidas en el RRI. En cualquier caso, a nadie escapa que las disposiciones más importantes para determinar los órganos competentes o la legislación aplicable en materia de contratos internacionales de consumo (en esencia,

[343] PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», cit., p. 206. Discutiendo la aplicación del artículo 29 LSSICE en materia de contratos electrónicos celebrados con consumidores, *vid.* Auto AP León núm. 474/2009, de 8 de octubre, F. J. 1º, y Auto AP Álava núm. 120/2010, de 15 de septiembre, F. J. 1º.

[344] Entre ellos, especialmente, DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 72 a 74.

[345] BOE núm. 157, de 2 de julio de 1985. Este artículo fue añadido en virtud del artículo único.9 LOMLOPJ (BOE núm. 174, de 22 de julio de 2015).

artículos 17 a 19 RBIbis[346]) no utilizan el lugar de celebración del contrato como criterio de conexión.

## IV. CONTRATACIÓN PRIVADA DOTADA DE FIRMA, EN AMBOS CASOS DE NATURALEZA ELECTRÓNICA: ASPECTOS LEGISLATIVOS PREVIOS

Una pieza central en nuestro estudio vendrá determinada por la necesidad de analizar, dentro de los contratos electrónicos, aquellos provistos de firma, firma que, como sabemos, no es, con carácter general, un elemento esencial determinante de la validez y eficacia de los mismos, pero sí un complemento fundamental a efectos de prueba de su contenido, autoría e integridad. Es por ello que un punto de partida adecuado con el que comenzar el análisis acerca de la influencia de la firma electrónica en la conclusión de contratos virtuales podría consistir (y así va a ser) en examinar el estado, previo y actual, de la regulación existente en la materia para, sobre esta base, diseccionar sus principales rasgos diferenciadores.

### 1. La Directiva europea sobre firma electrónica y su transposición al ordenamiento jurídico interno, español e italiano

Habida cuenta de la seguridad adicional que requiere el empleo efectivo de cuantas posibilidades comunicativas posibilita el uso de Internet, no es de extrañar que el sector de las firmas electrónicas fuera objeto de la regulación más temprana de entre el conjunto de actividades relacionadas con el comercio electrónico, tanto en el ámbito estatal como en el comunitario e internacional. En este punto, analizamos la normativa comunitaria originaria, plasmada en la DFE[347], y la incidencia que ha tenido en los sistemas jurídicos de nuestro país y de Italia, ambos pioneros (junto con Alemania) en la adopción de normas en materia de firma electrónica dentro de la UE. Para ello, y partiendo de un cuadro comparativo esencial sobre la equivalencia de estas normativas y de sus articulados (**anexo XIV**)[348], ponemos de relieve los aspectos más generales e importantes de cada uno de estos textos legales.

---

[346] DOUE L 351, de 20 de diciembre de 2012, p.1.

[347] DOCE L 13, de 19 de enero de 2000, p. 12.

[348] Por razones de lógica sistemática, el anexo XIV del presente estudio contiene, por lo que respecta al estado italiano, únicamente el Decreto Legislativo 10/2002 y el Decreto Legislativo actual (antes de las modificaciones últimas, operadas en 2016, como veremos en el apartado siguiente y en el anexo XV) 82/2005. Y ello porque, además de ser los más recientes y estrechamente vinculados con la DFE que nos sirve de referencia, permiten

Queda constatado cómo el comercio telemático requiere de firmas electrónicas y servicios conexos de autenticación de datos que posibiliten su idoneidad y operatividad. Sin embargo, desde un principio, la pluralidad normativa existente en materia de reconocimiento legal de firma electrónica y acreditación de los PSSIic entre los distintos Estados miembros presentaba el riesgo de obstaculizar gravemente el desarrollo de la más importante manifestación de este nuevo cauce de vehiculación de la voluntad negocial: la contratación electrónica. De ahí la necesidad de crear, a nivel europeo, un marco general claro sobre las condiciones aplicables a la firma electrónica que permitiera incrementar la confianza de los ciudadanos en las nuevas tecnologías de la información y de la comunicación, dotando de una eficacia pareja, equivalente a la tradicional, a los documentos rubricados electrónicamente y generando, a su vez, un sistema jurídico avalado por la existencia de entidades certificadoras que, permitiendo la expedición de firmas, garantizaran de forma fehaciente la titularidad, autenticidad e integridad de las transacciones a realizar[349].

Esta armonización e interoperabilidad jurídica tiene su primer reflejo en la DFE. Estructurada en un total de quince artículos, este texto es el resultado de un conjunto de acciones comunitarias previas en materia de firma electrónica, que nacen con un primer anuncio de propuesta legislativa sobre la materia, efectuado en una Comunicación, intitulada *El fomento de la seguridad y la confianza en la comunicación electrónica – Hacia un marco europeo para la firma digital y el cifrado*[350]. Poco después, el 1 de diciembre de 1997, el Consejo invita a la Comisión a que presente lo antes posible una propuesta de Directiva sobre firma electrónica[351], que daría

una comparativa visual más adecuada de los ordenamientos jurídicos español e italiano y de la relación, más o menos homogénea, que estos presentan con la norma comunitaria. Idénticas razones nos llevan a considerar, dentro del Decreto Legislativo 82/2005, tan sólo aquella parte que muestra interés a los efectos precitados, cual es la contenida en la Sección primera del Capítulo I, en las Secciones primera y segunda del Capítulo II y en el Capítulo VIII.

[349] PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», en ORDUÑA MORENO, F. J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, p. 500.

[350] COM (97) 503, de 8 de octubre de 1997.

[351] GARCÍA MÁS, F. J., «La contratación electrónica: la firma y el documento electrónicos», *Revista crítica de Derecho inmobiliario*, vol. 652, 1999, pp. 1 y ss.

lugar a la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica[352], y que, tras los Dictámenes del Comité Económico y Social[353], del Comité de las Regiones[354], del Parlamento Europeo[355], la Posición Común del Consejo[356] y la Decisión del Parlamento Europeo, dieron lugar a la Directiva propiamente dicha.

La DFE, en vigor desde la fecha de su publicación en el DOCE, el 19 de enero de 2000 (artículo 14), constituye un primer paso en la pretendida coherencia entre el Derecho de los Estados miembros en materia de firma electrónica. Sobre la base del principio, esencial en el ámbito de la contratación electrónica, de neutralidad tecnológica[357].

---

[352] DOCE C 325, de 23 de octubre de 1998, p. 5.

[353] DOCE C 40, de 15 de febrero de 1999, p. 29.

[354] DOCE C 93, de 6 de abril de 1999, p. 33.

[355] DOCE C 104, de 14 de abril de 1999, p. 49.

[356] DOCE C 243, de 27 de agosto de 1999, p. 83.

[357] Recogido, a los efectos que aquí interesan, en el considerando 8 DFE, este principio se traduce, en palabras de ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., p. 333, en la «[…] aptitud de las nuevas normas disciplinadoras del comercio electrónico para abarcar con sus reglas no sólo la tecnología existente en el momento en que se formulan sino también las tecnologías futuras sin necesidad de verse aquellas normas sometidas a su modificación»; en la misma línea, PÉREZ PEREIRA, M., *Firma electrónica: contratos y responsabilidad civil*, cit., p. 80, quien sostiene que «[e]l principio de neutralidad tecnológica se dirige fundamentalmente al legislador, dado que la finalidad de su aplicación es doble: haciendo normas que regulen la actividad "electrónica" (comercio, firma, protección de datos) sin aludir directamente a ninguna tecnología, se permite que la norma se pueda aplicar sea cual fuere el desarrollo tecnológico, sin que haya que modificar la norma cada vez que se produce un cambio de tecnología o innovación, y nunca se producirán lagunas en la aplicación de las normas si el conflicto se refiere a las medidas tecnológicas que han de tomarse. Así, si una norma jurídica es neutra desde el punto de vista tecnológico se está facilitando el empleo de tecnologías que vayan surgiendo con posterioridad a la promulgación de la norma, siempre y cuando cumplan unos requisitos establecidos en la norma, de tal manera que la seguridad jurídica sobre la validez del instrumento tecnológico permanece invariable», y VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 78 y 79, para el que «[l]a neutralidad tecnológica se basa en el carácter abstracto y general de la norma. Esto es, en la exigencia de que ninguna norma beneficie o se incline por la aplicación de una tecnología particular en la solución de un problema. En la práctica debe suponer que la ley no aluda a ninguna tecnología específica, sino que, por el contrario, incorpore todas las que existan en un momento determinado puedan existir en el futuro. Esto supondrá, además de no privilegiar a ningún titular concreto de derechos, que no sea necesario modificar la ley cada vez que aparezcan avances

La norma tiene por finalidad «[…] facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico»[358], creando, a tales efectos, un marco jurídico para dicha firma y para determinados servicios de certificación, con el fin de garantizar el correcto funcionamiento del mercado interior (artículo 1 DFE). Sin embargo, concluye el precepto (en línea con lo previamente dispuesto en el considerando 17), la DFE no regulará otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales, ni afectará a las normas y límites que rigen el uso de documentos, en aquellos casos en que existan requisitos, de forma o cualquier otro, establecidos en las legislaciones de los Estados miembros o en la misma normativa comunitaria; esta decisión, pensada para ser resuelta en la DCE, es tratada, sin embargo, tan sólo de manera somera y tangencial[359], sobre la base, en cualquier caso, del principio general de presunción y defensa de la validez de los actos y

tecnológicos». Su origen se encuentra en la LMCE, que no opta por ningún tipo de tecnología ni proceso técnico concreto; precisamente, en el precepto en el que define el concepto básico en torno al cual se construye toda la estructura de la Ley Modelo, como es el de *mensaje de datos* –artículo 2.a) LMCE–, se hace una formulación absolutamente abierta, que permite incluir en ella tanto los medios tecnológicos conocidos en el presente como aquellos otros que, de manera sucesiva, se vayan descubriendo e implementando en el futuro. Para alcanzar este fin se recurre a la institución jurídica de la *analogía*, de modo tal que, aludiéndose a medios conocidos en el momento actual, esta referencia se realiza como mención abierta, más a título de ejemplo que como lista cerrada. En concreto, sobre este principio se pronuncia de manera explícita el apartado octavo de la Guía para la incorporación al Derecho interno de la LMCE, y lo hace concluyendo con los siguientes términos: «[u]na de las características del comercio electrónico es la de que supone el empleo de mensajes programables, cuya programación en una terminal informática constituye el rasgo diferencial básico respecto de los documentos tradicionales consignados sobre papel. Todos estos supuestos están previstos por la Ley Modelo, que responde así a la necesidad en que se encuentran los usuarios del comercio electrónico de poder contar con un régimen coherente que sea aplicable a las diversas técnicas de comunicación que cabe utilizar indistintamente. Cabe señalar que, en principio, no se excluye ninguna técnica de comunicación del ámbito de la Ley Modelo, que debe acoger en su régimen toda eventual innovación técnica en este campo».

[358] No se precisa, añade su considerando 16, de «un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado celebrado entre un número determinado de participantes. En la medida en que lo permita la legislación nacional, ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas; no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales».

[359] PLAZA PENADÉS, J., «La firma electrónica (regulación en España y en la Unión Europea)», cit., p. 425.

negocios jurídicos realizados tecnológicamente[360]. Con posterioridad a la promulgación de la Directiva, se han dictado una serie de actos conexos importantes. Por orden cronológico se encuentra: en primer lugar, la DCMO[361]; en segundo lugar, la DPNRNPFE[362]; en tercer lugar, el IADFE[363], y, por último, la PAFE[364], conocido como *Plan de acción sobre la firma electrónica y la identificación electrónica para facilitar la prestación de servicios públicos transfronterizos en el mercado único*.

### 1.1. Evolución legislativa española

En nuestro país, la regulación inicial en materia de firma electrónica, certificados y PSSIic tuvo lugar merced al RDLFE [365], que, invocando (en mi opinión, erróneamente) razones de

[360] Desde una perspectiva internacional, la LMCE contemplaba ya el cumplimiento de los requisitos de firma por medio del empleo de medios electrónicos. En concreto, la posibilidad de que la exigencia legal de firma (típicamente manuscrita), pudiera verse satisfecha en su modalidad electrónica respecto de los mensajes de datos se previó, con carácter anticipado, en el artículo 7 de dicha Ley Modelo, que dio origen con posterioridad (también respecto de la DFE) a la LMFE, cuyo contenido refleja un creciente consenso internacional en materia de empleo de sistemas de acreditación y certificación para la atribución de una eficacia reforzada a las firmas electrónicas; para un estudio más extenso de ambas Leyes modelo, DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 119 a 122.

[361] DOCE L 289, de 16 de noviembre de 2000, p. 42.

[362] DOUE L 175, de 15 de julio de 2003, p. 45.

[363] COM (2006) 120 final. Indicando la aplicación por los países de la UE de los principios generales de la DFE, el Informe señalaba que la transposición de la Directiva al Derecho nacional de los Estados miembros permitió satisfacer la necesidad de reconocimiento jurídico de las firmas electrónicas, considerando, asimismo, alcanzados los objetivos de la norma.

[364] COM (2008) 798 final. A través de esta Comunicación, la Comisión propone un plan de acción cuyo objeto es ayudar a los países de la UE a aplicar soluciones de firma y de identificación electrónicas mutuamente reconocidas e interoperables, a fin de facilitar la prestación de servicios públicos transfronterizos en un contexto electrónico, evitando la fragmentación del mercado único. Las medidas de dicho plan se dividen en dos partes: de una parte, acciones concretas para mejorar la interoperabilidad transfronteriza de las firmas electrónicas reconocidas y de las firmas electrónicas avanzadas basadas en certificados cualificados; de otra, acciones para mejorar la interoperabilidad transfronteriza de la identidad electrónica.

[365] BOE núm. 224, de 18 de septiembre de 1999.

urgencia[366], fue aprobado, incluso, semanas antes que la versión definitiva de la DFE[367], colocándose a la cabeza de la UE en lo que a esta regulación se refería[368], pero originando, a cambio, un riesgo de descoordinación patente respecto de la pretendida armonización comunitaria[369].

---

[366] Como bien señala PLAZA PENADÉS, J., «La firma electrónica y su regulación en el Derecho español», en ORDUÑA MORENO, F. J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, p. 536, es criticable que la normativa sobre firma electrónica se aprobase a través de Decreto-ley, figura que está prevista, según el artículo 87 CE (BOE núm. 311, de 29 de diciembre de 1978), para casos de extraordinaria y urgente necesidad, «[…] circunstancia que evidentemente no se daba en la regulación de la firma electrónica, máxime, como ya se ha visto, cuando el Derecho español atribuía efectos a los documentos electrónicos acompañados de firma electrónica. Se trata de un costo más, como todos ellos desgraciado, de utilización inadecuada de los procedimientos constitucionales de elaboración de leyes a través de la figura del Decreto-ley, que, en este caso, como en todos, tiene como principal cometido eludir el debate y la confrontación de opiniones». En la misma línea, *vid.* GONZÁLEZ NAVARRO, F., «Comentario al art. 45 de la Ley de régimen jurídico de las Administraciones públicas y procedimiento administrativo común», *Estudios y comentarios legislativos (Civitas)*, vol. 1, 2007, p. 15; MARTÍNEZ NADAL, A., «Comentarios de urgencia al urgentemente aprobado Real Decreto-ley 14/1999 de 17 de septiembre, sobre firma electrónica», *La ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*, vol. 6, 1999, pp. 1860 a 1871; MORENO DELGADO, M./SAN MARTÍN SEGURA, D., «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja*, vol. 2002, p. 214.

[367] EL RDLFE fue convalidado por la RACRDLFE (BOE núm. 257, de 27 de octubre de 1999).

[368] FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, Madrid, Reus, 2006, p. 19; GARCÍA MÁS, F. J., «La contratación electrónica: la firma y el documento electrónicos», cit., p. 774; GUILLÉN CATALÁN, R., «La protección jurídica de los consumidores ante el envío de comunicaciones comerciales por vía electrónica», en PLAZA PENADÉS, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, p. 158.

[369] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 124. Cuestionando el carácter urgente de la norma, *vid.* ALAMILLO DOMINGO, I./URIOS APARISI, X., «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», *Revista de la contratación electrónica*, vol. 46, 2004, p. 3; BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., pp. 399 y 400; HUERTA VIESCA, M. I., «La firma electrónica en la regulación española: valoración crítica», en HUERTA VIESCA, M. I./RODRÍGUEZ RUIZ DE VILLA, D. (coords.) *Los prestadores de servicios de certificación en la contratación Electrónica*, Cizur Menor, Aranzadi, 2001, p. 21; MARTÍNEZ NADAL, A., *La Ley de firma electrónica*, Madrid, Civitas, 2000, pp. 15 y 16 y 312 y 313. Para un estudio más profundo del Real Decreto-ley, *vid.* ALCOVER GARAU, G., «El Real Decreto-ley sobre la firma electrónica», *Revista de la contratación electrónica*, vol. 1, 2000, pp. 7 a 27; BATUECAS CALETRÍO, A., «Hacia una ley de firma electrónica que mejore el Real Decreto-ley de firma

No obstante, con anterioridad a esta norma y de manera ciertamente sectorial y dispersa, el ordenamiento jurídico español ya contaba con un entramado de normas legales y de disposiciones de rango inferior a la Ley que sostenían la validez y eficacia de la firma electrónica[370]; como principales, en primer lugar, se encuentra la LOPJ, cuyo artículo 230.1 sostenía que, en materia judicial, los Juzgados y Tribunales podrán utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establece la (ya derogada) LOTADCP[371]; en segundo lugar, la (también derogada) LMV[372], reguladora de las operaciones de Bolsa mediante el conocido como *Sistema de Interconexión Bursátil*, integrado, como señala la propia Exposición de Motivos de la Ley, mediante una red informática, donde se debe encuadrar el ACCNMVIS[373]; en tercer lugar, el artículo 45.5 de la, también, ya abolida, LRJAP-PAC[374], que establecía que «[l]os documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones públicas, o los que éstas emitan como copias originales almacenados por estos mismos medios, gozarán de

electrónica 14/1999, de 17 de septiembre», en APARICIO VAQUERO, J. P./MORO ALMARAZ, M. J./BATUECAS CALETRÍO, A. (coords.) *Internet y comercio electrónico*, Salamanca, Universidad de Salamanca, 2002, pp. 153 a 176; FERNÁNDEZ DOMINGO, J. I., «La contratación electrónica y el Real Decreto-ley 14/1999 sobre firma electrónica», *Actualidad civil*, vol. 2, 2000, pp. 527 a 548; GARCÍA AGUILAR, N., «El Real Decreto-ley 14/1999 sobre firma electrónica», *Revista internauta de práctica jurídica*, vol. 4, 2000, pp. 1 a 16; GARCÍA MÁS, F. J., «La firma electrónica Directiva 1999/93/CE, de 13 de diciembre de 1999 y Real Decreto-ley 14/1999 de 17 de septiembre», *Notariado y contratación electrónica*, vol. 1, 2000, p. 96; ILLESCAS ORTIZ, R., «La firma electrónica y el Real Decreto-ley 14/1999 de 17 de septiembre», *Derecho de los negocios*, vol. 109, 1999, pp. 1 a 14; MORENO DELGADO, M. Y OTROS, «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», cit., pp. 1 a 19.

370 *Vid.* GARCÍA MÁS, F. J., «La contratación electrónica: la firma y el documento electrónicos», cit., pp. 774 y 775; MARTÍNEZ NADAL, A., *La Ley de firma electrónica*, cit., pp. 23 a 25; PLAZA PENADÉS, J., «La firma electrónica y su regulación en el Derecho español», cit., pp. 531 y 532.

371 BOE núm. 262, de 31 de octubre de 1992. La derogación se produce en virtud de letra a) de la D. D. Única LOPDCP.

372 BOE núm. 181, de 29 de julio de 1988. La derogación se produce en virtud de letra a) de la D. D. Única del TRLMV (BOE núm. 255, de 24 de octubre de 2015).

373 En la actualidad, merced al ACCNMVAS (BOE núm. 292, de 5 de diciembre de 2011).

374 BOE núm. 285, de 27 de noviembre de 1992. La derogación se produce en virtud de letra a) del apartado 2 de la D. D. Única de la LPACAP (BOE núm. 236, de 2 de octubre de 2015).

la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras Leyes»[375]; en cuarto lugar, la redacción primigenia del artículo 82.2.1º de la LIVA[376], que disponía que «[l]a repercusión del impuesto deberá efectuarse mediante factura o documento análogo, que podrán emitirse por vía telemática, en las condiciones y con los requisitos que se determinen reglamentariamente»[377], y, por último, la OORVPBM[378],cuya D. A., apartado sexto, autoriza a la DGRN «[…] a aprobar modelos en soporte informático o con firma electrónica, siempre que se garantice la identidad indubitada de los contratantes y la integridad e inalterabilidad del documento».

La norma, en vigor desde el 19 de septiembre de 1999 (D. F. 3ª), se estructura en un total de cinco títulos (Título I, intitulado *disposiciones generales*, que contiene un único capítulo, del mismo nombre –artículos 1 a 3–; Título II, bajo la denominación *la prestación de servicios de certificación*, que consta de un Capítulo primero sobre *principios generales* –artículos 4 a 7–, de un Capítulo segundo sobre *certificados* –artículos 8 a 10–, de un Capítulo tercero sobre *condiciones exigibles a los prestadores de servicios de certificación* –artículos 11 a 15– y de un último Capítulo cuarto sobre *inspección y control de la actividad de los prestadores de servicios de certificación* –artículos 16 a 18–; Título III, regulador de *los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable*, comprensivo de un Capítulo único, del mismo nombre –artículos 19 a 22–; Título IV, que trata la *tasa por el reconocimiento de acreditaciones y certificaciones*, y que incluye un solo capítulo, de idéntico nombre –artículo 23–, y Título V, para *infracciones y sanciones*, que

[375] Esta disposición fue desarrollada por el RDUTEITAGE (BOE núm. 52, de 29 de febrero de 1996).

[376] BOE núm. 312, de 29 de diciembre de 1992.

[377] Este precepto, desarrollado por mor del artículo 9 bis RDDEEFIEP (BOE núm. 312, de 30 de diciembre de 1985) y aplicado gracias a la ONASFT (BOE núm. 77, de 29 de marzo de 1996), ha experimentado dos cambios en su redacción: una primera, en la que se modifican los apartados 2 y 3 por el artículo 4.9 de la TLMFAOS (BOE núm. 313, de 31 de diciembre de 2002), desapareciendo la referencia a la telemática que aquí nos interesa; una segunda, en la que se modifican de nuevo los mismos apartados, esta vez en virtud del artículo 67.1 LPGE (BOE núm. 312, de 28 de diciembre de 2012). En la actualidad, la factura electrónica se encuentra regulada en la LIFE-CRCFSP (BOE núm. 311, de 28 de diciembre de 2013), a la que se remite (junto con el resto de normas tributarias en materia de emisión de facturas por vía electrónica) la D. A. 7ª LFE. Sobre la factura electrónica, *vid.* ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 198 y 199.

[378] BOE núm. 172, de 20 de julio de 1999.

igualmente contempla un capítulo, del mismo nombre –artículos 24 a 26–), una D. A. Única (*posibilidad de emisión por las entidades públicas de radiodifusión de una Comunidad Autónoma en el territorio de otras con las que aquélla tenga espacios radioeléctricos colindantes*), una D. T. Única (*prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de este Real Decreto-ley*) y tres D. F. (*fundamento constitucional*, *habilitación al Gobierno* y *entrada en vigor*). Con posterioridad a su promulgación, se publicó, como normativa adicional, la ORAPSSIisc[379], en desarrollo de los artículos 6 y 22 RDLFE (artículo único).

El objeto del RDLFE no es otro que el de regular «el uso de la firma electrónica[380], el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación» por parte de PSSIic establecidos en España (artículo 1).

Son estos prestadores los obligados a cumplir los requisitos legales necesarios para desarrollar su actividad en nuestro país, determinando, de un lado, el tipo de PSSIic de que se trate y, de otro, el tipo de firma electrónica expedida, la mayor o menor eficacia jurídica de los certificados electrónicos emitidos. Pese a todo, las carencias (formales, como hemos visto, pero también de contenido[381]) que presentaba el texto propiciaron la promulgación de la

[379] BOE núm. 45, de 22 de febrero de 2000.

[380] Como bien indica MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, Cizur Menor, Aranzadi, 2004, pp. 40 y 41, con esta previsión general, la LFE (al igual que el RDLFE y la DFE) pretende regular la firma electrónica en general y no sólo los usos comerciales de la misma; por tanto, su ámbito de aplicación «[…] sería no sólo el comercio electrónico en sentido estricto sino también todas aquellas comunicaciones de datos realizadas por medios electrónicos, y no necesariamente comerciales, que, con frecuencia, y de forma entendemos que incorrecta, se incluyen dentro del concepto de comercio electrónico en sentido amplio».

[381] Entre otras, como expone DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 124, «[…] el gravoso régimen de responsabilidades, infracciones y sanciones previsto para los prestadores de servicios de certificación; la imposición de cargas o costes que menoscaban el empleo generalizado de la firma electrónica así como que el sistema instaurado aparecía caracterizado por una excesiva intervención administrativa, en el que la atribución de una especial eficacia jurídica a las firmas electrónicas se hacía depender del cumplimiento de un complejo entramado jurídico-público, en el que el resto de modalidades de firma electrónica tenían un valor práctico muy limitado (la firma electrónica no avanzada y el certificado no reconocido constituyen categorías legales de muy escaso valor práctico); y el gravoso régimen de responsabilidad de los prestadores de servicios de certificación (como la tasa fijada por el reconocimiento de acreditaciones y certificaciones y la obligación de las entidades de evaluación de abonar los gastos originados por la evaluación realizada para su acreditación)». También BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de

LFE[382], que llevó a cabo, ahora sí, la transposición al ordenamiento jurídico español de la DFE[383] y, por consiguiente, la derogación del RDLFE «[…] y cuantas disposiciones de igual o inferior rango se op[usieran] a lo dispuesto en esta ley» (D. D. Única LFE). Se conseguía, de este modo, una mayor transparencia en la tramitación y el debate de una materia de especial trascendencia, como es la firma electrónica[384], aportando, además, una revisión de la terminología, una modificación de la sistemática y una simplificación del texto, «[…] facilitando

diciembre, de firma electrónica», cit., p. 399, quien, pese a subrayar la valoración positiva inicial que mereció la norma, pues «[…] resultó esencial para fomentar el progreso de las transacciones electrónicas en España, para la difusión del concepto de firma electrónica», puso de manifiesto su falta de desarrollo completo, quedando pendiente, entre otras materias, la acreditación de PSSIic, la certificación de dispositivos o el registro de prestadores, propiciando, todo ello, su escasa aplicación efectiva y utilidad real.

[382] Para un análisis pormenorizado de la LFE, *vid.*, entre otros, ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 89 a 108; MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., pp. 1 y ss.; RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, Madrid, Consejo General del Notariado, 2004, pp. 1 y ss. Para un estudio crítico de la norma, *vid.* ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., pp. 1 y ss.

[383] El motivo de la derogación del RDLFE en detrimento de la LFE se explica en el apartado primero de la Exposición de Motivos de la norma: «[e]l Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, fue aprobado con el objetivo de fomentar la rápida incorporación de las nuevas tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las empresas, los ciudadanos y las Administraciones públicas. De este modo, se coadyuvaba a potenciar el crecimiento y la competitividad de la economía española mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización de transacciones electrónicas en redes abiertas como es el caso de Internet. El citado real decreto ley incorporó (*error, por cuanto hemos explicado anteriormente*) al ordenamiento público español la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, incluso antes de su promulgación y publicación en el Diario Oficial de las Comunidades Europeas. Tras su ratificación por el Congreso de los Diputados, se acordó la tramitación del Real Decreto Ley 14/1999 como proyecto de ley, con el fin de someterlo a una más amplia consulta pública y al posterior debate parlamentario para perfeccionar su texto. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000. Esta ley, por tanto, es el resultado del compromiso asumido en la VI Legislatura, actualizando a la vez el marco establecido en el Real Decreto Ley 14/1999 mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor tanto en nuestro país como en el ámbito internacional» (la cursiva y los paréntesis son propios).

[384] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 28.

su comprensión y dotándolo de una estructura más acorde con nuestra técnica legislativa» (apartado III de la Exposición de Motivos de la LFE)[385].

La nueva Ley, cuya entrada en vigor se produjo a los tres meses de su publicación en el BOE (esto es, el 20 de marzo de 2004, tal y como establece la D. F. 3ª LFE[386]), está integrada en su mayor parte por reglas administrativas y de intervención pública en la actividad de firma electrónica[387]. Se estructura en un total de treinta y seis artículos, repartidos en cinco títulos: Título I, intitulado *disposiciones generales* –artículos 1 a 5–, que contiene los principios generales

[385] Hablando, incluso, con carácter previo, del Borrador del Anteproyecto legislativo, autores como GALINDO AYUDA, F., «Comentarios al Borrador de Anteproyecto de Ley de firma electrónica», *La ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*, vol. 2, 2002, p. 1748, señalaban ya que los nuevos preceptos proyectados «[…] concretan, aclaran, delimitan y complementan la regulación existente sobre firma electrónica».

[386] Según BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., pp. 398 y 399, esta *vacatio legis* responde, seguramente, a «[…] la necesaria adaptación de todos los agentes afectados por la norma a los notables cambios que se contienen en la misma y a las disposiciones novedosas que viene a introducir en lo que constituye el procedimiento de autenticación electrónica». En la misma línea, GÁLLEGO HIGUERAS, G. F., «Comentarios a la reciente Ley 59/2003, de 19 de diciembre, de firma electrónica: algunas novedades al marco regulador existente», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 6, 2004, p. 22.

[387] ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 91 y 92, lo expresa, al hablar de la estructura de la LFE, en los siguientes e interesantes términos: «[c]ualquier lector avezado aprecia en seguida que dos grandes categorías de preceptos se incluyen en la norma. De una parte existen disposiciones de carácter sustantivo o material, ocasionalmente acompañadas de alguna referencia procesal, y de otra se contienen reglas de pura índole administrativa. Éstas son amplia mayoría como ya se ha podido inferior de los rótulos de los diversos títulos: en realidad ya en el artículo 4 y hasta el final de la norma, con alguna excepción, el lector halla predominantemente reglas administrativas y de intervención pública en el mercado de la certificación de firmas electrónicas principalmente. A pesar de ello no puede en modo alguno afirmarse que estemos ante una norma pura de Derecho administrativo: las disposiciones sustantivas contenidas son de trascendencia jurídica elevada. Y no sólo para las relaciones jurídico-privadas de los empresarios entre sí (relaciones *business to business*) y entre éstos y los consumidores (relaciones *business to consumers*) sino también para las relaciones civiles entre los ciudadanos y para las relaciones entre los ciudadanos y las Administraciones públicas. No estamos por consiguiente ante una norma destinada en exclusiva a reglar el comercio electrónico sino a reconocer jurídicamente un nuevo soporte, distinto del oral o del escrito (*error de concepto este, en mi opinión, como ya hemos tenido ocasión de fundamentar*), hábil para la emisión de declaraciones de voluntad y de ciencia por parte de las personas. Ésta es, en efecto, la segunda dicotomía que puede advertirse en la parte dispositiva de la LFE: normas materiales y normas de intervención administrativa de una parte, normas tanto para las relaciones privadas como para las relaciones jurídico-públicas por otra».

que delimitan los ámbitos subjetivo y objetivo de aplicación de la LFE, los efectos de la firma electrónica, el régimen de empleo ante las Administraciones públicas y el acceso a la actividad de los PSSIic; Título II, que, regulador de los *certificados electrónicos*, se estructura en tres capítulos, el primero sobre *disposiciones generales* acerca de quiénes pueden ser los titulares de estos certificados y de las vicisitudes que afectan a su vigencia –artículos 6 a 10–, el segundo sobre *certificados reconocidos* –artículos 11 a 14– y el tercero sobre *el documento nacional de identidad electrónico* –artículos 15 y 16–; Título III, que disciplina la *prestación de servicios de certificación*, y lo hace a través de dos capítulos, el primero sobre las *obligaciones* a que están sujetos los PSSIic, distinguiendo con nitidez aquellas que solamente afectan a los que expiden certificados reconocidos –artículos 17 a 21–, y el segundo sobre el régimen de *responsabilidad* aplicable –artículos 22 y 23–; Título IV, relativo a los requisitos que deben reunir los *dispositivos de* creación y verificación de *firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica*, bifurcado en un primer capítulo, sobre *dispositivos de firma electrónica* –artículos 24 y 25–, y en un segundo capítulo, que trata de las cuestiones relativas a la *certificación de prestadores de servicios de certificación y de dispositivos de creación de firma electrónica* –artículos 26 a 28–; Título V, concerniente a la *supervisión y control* de los PSSIic –artículos 29 y 30–, y, por último, Título VI, para las *infracciones y sanciones* en que se incurra como consecuencia del incumplimiento de la norma –artículos 31 a 36–. A ello se añaden once D. A. (*fe pública y uso de firma electrónica*; *ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica*; *expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias*; *prestación de servicios por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda*; *modificación del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social*; *régimen jurídico del documento nacional de identidad electrónico*; *emisión de facturas por vía electrónica*; *modificaciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*; *garantía de accesibilidad para las personas con discapacidad y de la tercera edad*; *modificación de la* Ley de *Enjuiciamiento Civil,* y *resolución de conflictos*), dos D. T. (*validez de los certificados electrónicos expedidos previamente a la entrada en vigor de esta ley* y *prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley*), una D. D. (*derogación normativa*) y tres D. F. (*fundamento constitucional*, *desarrollo reglamentario* y *entrada en vigor*). Con posterioridad a su entrada en vigor, tendrá

lugar la publicación, como normativa complementaria, de la OTECE[388] y del RDEDNI-CFE[389].

Con la finalidad de propiciar la expansión de la firma electrónica como instrumento capaz de generar confianza en las transacciones telemáticas, agilizando el comercio electrónico y confiriendo seguridad a las comunicaciones efectuadas a través de Internet, la LFE tiene como objeto esencial la regulación de la firma electrónica, su eficacia jurídica y la prestación de SSIisc[390], todo ello sin alterar «[…] las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten» (artículo 1 LFE, en línea con el artículo 1.2.1º RDLFE). Al igual que la DFE en la que se inspira, la Ley regula la utilización de la firma electrónica en general, no sólo los aspectos relativos a sus usos comerciales, de modo que también abarca todas aquellas comunicaciones de datos efectuadas por medios electrónicos, como pudieran ser las actuaciones con las Administraciones públicas[391].

La norma introduce ciertas modificaciones sustanciales respecto del cuerpo precedente[392], entre las que destaca la creación de una regulación concreta para el uso de firmas electrónicas por parte de personas jurídicas; el acogimiento explícito de las relaciones de representación que puedan subyacer en el empleo de la firma electrónica; la adición de un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica, a los solos efectos de su utilización en el ámbito tributario; la incorporación del término *firma electrónica reconocida* para aludir a aquella que se equipara legalmente a la firma manuscrita; la

---

388 BOE núm. 246, de 12 de octubre de 2004.

389 BOE núm. 307, de 24 de diciembre de 2005.

390 No obstante, autores como ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 16, propusieron en su momento una redacción distinta para el artículo 1.1 LFE: «[e]sta Ley regula la firma electrónica, su eficacia jurídica *general, las bases del empleo de la firma electrónica por las Administraciones Públicas,* la prestación de servicios de certificación *y aprueba el Documento Nacional de Identidad electrónico*» (en cursiva aparece aquella parte adicional a la recogida finalmente en la norma).

391 MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», cit., p. 225.

392 Estas modificaciones se contienen en el mismo texto de la LFE, concretamente en el apartado III de su Exposición de Motivos. Sobre esta cuestión, *vid.* DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., pp. 526 y 527.

incorporación al DNI de facilidades de identificación y de firma electrónica, previendo de manera expresa la existencia de un DNIe, que surtirá plenos efectos en orden a la integridad y autenticidad de las comunicaciones electrónicas que a través de él se lleven a cabo[393]; el incremento de la relevancia del sector privado y de la autorregulación en los sistemas de certificación de los PSSIic, propiciando, con ello, el desarrollo de sistemas voluntarios de acreditación; el reforzamiento de las capacidades de inspección y control sobre estos prestadores de servicios de certificación; la eliminación de determinados aspectos administrativos, como el registro de PSSIic, que es sustituido por un simple servicio de difusión de información sobre estos prestadores, sobre las certificaciones de calidad y sobre las características de los productos y servicios con que cuentan para el desarrollo de su actividad, o, en fin, la aclaración de las garantías económicas que han de prestar los PSSIic que emitan certificados reconocidos[394].

### 1.2. Principales normas italianas en materia de firma electrónica

Al igual que en España, antes de la publicación oficial de la DFE, Italia también había procedido ya a elaborar leyes en materia de firma electrónica[395]. La normativa más relevante

---

[393] Como en su momento apuntara DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 125, «[…] la implantación plena de este instrumento debería facilitar la generalización del uso de firmas electrónicas, así como un aumento de las posibilidades de ciertas actividades a través de Internet, en la medida en que contribuye a hacer posible la determinación de la identidad o características personales de quien se encuentra conectado a la Red. Este cambio puede aportar más confianza y seguridad para el desarrollo de ciertos modelos de negocio, por ejemplo, al facilitar una vía de comprobación en línea de que quien contrata el acceso a ciertos contenidos reúne las circunstancias personales exigidas; por ejemplo, ser mayor de edad para visualizar ciertos contenidos, cuya difusión entre menores puede incluso estar considerada como un delito». Para el desarrollo de esta cuestión, se dictó el antes mencionado RDEDNI-CFE. Sobre este asunto, MARTÍNEZ NADAL, A., «Firma electrónica, certificados y entidades de certificación», *Revista de la contratación electrónica*, vol. 68, 2006, pp. 41 a 64.

[394] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 124 y 125.

[395] Sobre la evolución de la legislación italiana en materia de firma electrónica, *vid.* BUONOMO, G./MERONE, A., «La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio (alla luce delle modifiche introdotte dalla l. 221/2012)», *Judicium: il processo civile in Italia e in Europa*, vol. 1, 2013, pp. 2 a 10; CARLONI, E., «Tendenze recenti e nuovi principi della digitalizzazione pubblica», *Giornale di Diritto amministrativo: mensile di legislazione, giurisprudenza, prassi e opinioni*, vol. 2, 2015, pp. 148 a 158; CIACCI, G., *La firma digitale*, cit., pp. 107 a 192; CLARIZIA, R., *I contratti informatici*, cit., pp. 119 a 121; COMANDÉ, G./SICA, S., *Il commercio elettronico: profili giuridici*, Turín, Giappichelli, 2001, pp. 126 y 127 y 143 a 160; DI COCCO, C. Y OTROS,

sobre la materia está constituida, en primer lugar, por la por el artículo 15, *comma* 2, LPASA[396], que introduce en el ordenamiento jurídico italiano el principio general de la validez y relevancia jurídica de las representaciones informáticas, disponiendo literalmente que «[…] los actos, datos y documentos elaborados por la Administración pública y por los particulares con instrumentos informáticos o telemáticos, los contratos celebrados del mismo modo, así como su almacenamiento y transmisión con instrumentos informáticos, son válidos y relevantes a todos los efectos legales. Los criterios y las modalidades de aplicación del presente apartado se establecerán, para la Administración pública y para los particulares, con específicas normas a adoptar dentro de los ciento ochenta días desde la entrada en vigor de la presente Ley con arreglo al artículo 17, apartado 2, LDAGOPCM[397] (*abreviatura propia*)[398]. Los esquemas de las normas se comunicarán a la Cámara de Diputados y al Senado de la República para la obtención del parecer de las pertinentes Comisiones»[399]. Esta norma no nace para disciplinar el comercio electrónico y, por tanto, con fines jurídico-privados; antes al contrario, está pensada para posibilitar la transmisión de actos jurídicos virtuales por parte de la Administración pública.

En aplicación y desarrollo del precepto anterior, fue promulgado el DPRDSIT[400]. Esta disposición, que se estructura en un total de tres capítulos (Capítulo I, sobre *principios generales*

*Temi di Diritto dell'informatica*, cit., pp. 49 a 69; FINOCCHIARO, G. D., «La firma digitale: formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici», en F., G. (coord.) *Commentario del Codice civile Scialoja-Branca*, Bolonia, Zanichelli, 2000, pp. 1 a 214; PARISI, F., *Il contratto concluso mediante computer*, Padua, Cedam, 1987, pp. 51 a 84; ROSELLO, C./FINOCCHIARO, G. D./TOSI, E., *Commercio elettronico, documento informatico e firma digitale: la nuova disciplina*, Turín, Giappichelli, 2003, pp. 531 a 549; SOLDATI, N., «La stipulazione on-line dei contratti commerciali», en AA.VV. (coord.) *Studi di diritto dell'economia e dell'impresa in memoria di Antonio Cicognani*, Padua, Cedam, 2012, pp. 609 a 652.

396 Gazzetta Ufficiale num. 63, 17 marzo 1997.

397 Gazzetta Ufficiale num. 214, 12 settembre 1988.

398 La cursiva y los paréntesis son propios.

399 Sobre esta norma, *vid.* FINOCCHIARO, G. D. Y OTROS, *Diritto dell'informatica*, cit., p. 119; ROSELLO, C. Y OTROS, *Commercio elettronico, documento informatico e firma digitale: la nuova disciplina*, cit., pp. 531 a 534.

400 Gazzetta Ufficiale num. 60, 13 marzo 1998. Esta norma responde, como bien señala DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 115 y 116, a un modelo regulatorio «[…] reglamentista, al atribuir reconocimiento legal en determinadas a una modalidad específica de creación de firma electrónica –basada en el uso

–artículos 1 a 9–; Capítulo II, sobre *firma digital* –artículos 10 a 19–, y Capítulo III, para las *normas de actuación* –artículos 20 a 22–), reconoce las modalidades concretas de actuación del principio general consagrado en la LPASA, optando decididamente por la técnica de la firma digital basada en la criptografía asimétrica[401], además de fijar los criterios de equivalencia entre documento escrito y documento informático y entre firma autógrafa y firma digital, si bien con algunas limitaciones y precisiones[402]. Ulteriormente, este texto será derogado por el DPRDA[403], y que, al igual que el DPRDSIT, remite a las reglas técnicas, emanadas con el DPCMDI[404].

Con posterioridad, y con el propósito de implementar la DFE, emana el DLDFE[405], comprensivo de un total de trece preceptos. Esta nueva norma se basa, fundamentalmente, en dos aspectos esenciales: de un lado, introduce la *firma electrónica* y la *firma electrónica avanzada*, para cuyas definiciones se remite a la transposición efectuada; de otro, establece el libre acceso al mercado de los PSSIic. Asimismo, el DLDFE modificará las disposiciones en materia de prueba, ya reformadas por el DPRDA. El artículo 13 DLDFE preveía cambios en la normativa, disponiendo que, dentro de los treinta días desde la fecha de su entrada en vigor, se publicará un reglamento a los efectos del artículo 17, apartado 2, LDAGOPCM, que posibilitará la coordinación de las disposiciones del texto único emanado con el DPRDA con las

---

de la criptografía asimétrica de clave pública–, regular en detalle los requisitos a los que se subordina el funcionamiento de las entidades de certificación así como su régimen de responsabilidad, y atribuir derechos y obligaciones a los titulares de las claves». Para un análisis de esta norma y de las disposiciones de desarrollo, *vid.* FINOCCHIARO, G. D., «La firma digitale: formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici», cit., 1 y ss.

[401] Para un estudio más exhaustivo de la firma digital y de su importancia en el ordenamiento jurídico italiano, *vid.* FINOCCHIARO, G. D., «Documento informatico e firma digitale», *Contratto e impresa*, vol. 2, 1998, p. 956.

[402] ROSELLO, C. Y OTROS, *Commercio elettronico, documento informatico e firma digitale: la nuova disciplina*, cit., p. 534.

[403] Gazzetta Ufficiale num. 42, 20 febbraio 2001. Ambas normas son sustancialmente convergentes, si bien el DPRDA introduce importantes modificaciones respecto del DPRDSIT. Entre ellas, la más relevante es la concerniente a la eficacia probatoria de la firma digital, antes disciplinada en el artículo 5 DPRDSIT y ahora en el artículo 10 DPRDA.

[404] Gazzetta Ufficiale num. 87, 15 aprile 1999.

[405] Gazzetta Ufficiale num. 39, 23 gennaio 2002.

indicaciones del presente Decreto Legislativo y de la DFE, así como la fijación de los requisitos necesarios para el desarrollo de la actividad de los PSSIic. El apartado segundo precisará que el texto será emanado a propuesta y con el concierto de los ministros indicados en el artículo 1.2º LAICE[406].

Por su parte, el DPRFE[407], con un total de diecisiete artículos, presenta un doble objetivo: en primer lugar, coordinar las disposiciones del DPRDA (de origen íntegramente nacional) sobre firma digital y las normas del DLDFE (de derivación europea) en materia de firma electrónica, coordinando las dos tipologías de firma informática existentes y los dos cuerpos normativos que hasta entonces las disciplinaban, para lo cual define cuatro tipos de firma: la firma electrónica general, la firma electrónica avanzada, la firma electrónica cualificada y la firma digital; en segundo lugar, especificar los nuevos requisitos para el desarrollo de la actividad de los PSSIic, distinguiendo entre prestadores *acreditados* y *cualificados*. La precitada coordinación fue operada por el DLDFE, modificando, pues, el DPRDA.

Por último, se encuentra el, actualmente vigente, CAD[408], que propone, ante todo, la aseguración por el Estado, las Regiones y las Autonomías locales de la disponibilidad, la gestión, el acceso, la transmisión, la conservación y la utilización de la información en su modalidad digital, así como la organización y actuación a tales fines utilizando, con las modalidades más apropiadas, las tecnologías de la información y de la comunicación (artículo 2.1). En concreto, este Código persigue corregir y coordinar los aspectos civiles y procesales relativos al valor del documento informático, así como difundir el uso de los nuevos avances informáticos entre los ciudadanos y las empresas; tal objetivo, podemos decir, se entiende tan sólo parcialmente alcanzado, dado que, desde un punto de vista formal, permanecen disposiciones fuera del texto (como el DPRDA, a menudo inútilmente repetido por no estar completamente derogado) que lo integran de modo imperfecto o no conclusivo[409]. En todo caso, con

[406] Gazzetta Ufficiale num. 16, 20 gennaio 2001.

[407] Gazzetta Ufficiale num. 138, 17 giugno 2003.

[408] Gazzetta Ufficiale num. 112, 16 maggio 2005.

[409] Numerosa es la doctrina que se ha pronunciado respecto de este Código. Entre ella, destacan CAVALLONI, A., *Il contratto telematico: profili generali*, Padua, Cedam, 2013, pp. 176 a 178; DE MURI, L., «Gli aspetti legali e contrattuali del commercio telematico», en AA.VV. (coord.) *Commercio elettronico*, Milanofiori Assago, Wolters Kluwer, 2014, pp. 27 a 29; FIORELLI, G. I., *Il contratto elettronico tra armonizzazione materiale e Diritto internazionale privato*, cit., pp. 114 a 116; LISI, A./GIACOPUZZI, L., *Guida al Codice dell'amministrazione digitale: con focues su*

carácter posterior a su promulgación, se han sucedido diversas modificaciones de la norma, personificadas, en primer lugar, en el DLCAD[410]; en segundo lugar, en el DLAPIN[411]; en tercer lugar, en el PDLMICAD[412]; en cuarto lugar, en el DLUM[413], coordinado con la LUMUCP[414], y, en quinto y último lugar, en el DPCMFEA[415].

Su estructura consta de ocho capítulos: un Capítulo I, sobre *principios generales*, que se subdivide, a su vez, en tres secciones (Sección I, que contiene *definiciones, finalidad y ámbito de aplicación* de la norma –artículos 1 y 2–; Sección II, que versa sobre los *derechos de los ciudadanos y de las empresas* –artículos 3 a 11–, y Sección III, que regula la *organización de las Administraciones públicas* y las *relaciones entre Estado, Regiones y Autonomías locales* –artículos 12 a 19–); un Capítulo II, para todo aquello relacionado con el *documento informático y* las *firmas electrónicas*, así como con los *pagos, libros y escrituras*, dividido también en tres secciones (Sección I, para el *documento informático* propiamente dicho –artículos 20 a 23–; Sección II, que disciplina las *firmas electrónicas y* los *prestadores de servicios de certificación* –artículos 24 a 37–, y Sección III, para los *contratos, pagos, libros y escrituras* –artículos 38 y 39–); un Capítulo III, relativo a la *formación, gestión y*

*archiviazione e fatturazione elettronica*, Matelica, Halley, 2006, p. 12; MARTONI, M., *Firme elettroniche: profili informatico-giuridici*, Roma, Aracne, 2010, pp. 77 a 116.

410 Gazzetta Ufficiale num. 99, 29 aprile 2006.

411 Gazzetta Ufficiale num. 166, 19 luglio 2010. Antes del DLAPIN, los actos públicos estaban excluidos de la forma electrónica, pero sus copias podían, sin embargo, cumplir «[…] la obligación del registro, de la transcripción, de la inscripción, de la anotación de los registros inmobiliarios y de la cesión catastral con procedimiento telemático» (artículo 1 DPRAI –Gazzetta Ufficiale num. 254, 30 ottobre 2000–).

412 Gazzetta Ufficiale num. 6, 10 gennaio 2011. Sobre el PDLMICAD, *vid.* FINOCCHIARO, G. D., «Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale», *Contratto e impresa*, vol. 2, 2011, pp. 495 y ss.; FINOCCHIARO, G. D., «Le copie per immagine su supporto informatico avranno l'efficacia probatoria degli atti originali», *Guida al Diritto*, vol. 8, 2011, pp. 62 y ss.; MACRÌ, I./MACRÌ, U./PONTEVOLPE, G., *Il nuovo Codice dell'amministrazione digitale: le tecnologie informatiche e le norme che ne disciplinanol'uso, aggiornate al D.Lgs. n. 235/2010*, Milanofiori Assago, Wolters Kluwer, 2011, pp. 1 y ss. Tanto el DLAPIN como el PDLMICAD responden a la previsión contenida en la LSESCPC (Gazzetta Ufficiale num. 140, 19 giugno 2009), sobre *Disposizioni per lo sviluppo economico, la semplificazione, la competitività nonché in materia di processo civile*.

413 Gazzetta Ufficiale num. 245, 19 ottobre 2012.

414 Gazzetta Ufficiale num. 294, 18 dicembre 2012.

415 Gazzetta Ufficiale num. 117, 21 maggio 2013.

*conservación de los documentos informáticos*, comprensivo de los artículos 40 a 44; un Capítulo IV, para las *transmisiones informáticas de documentos* (artículos 45 a 49); un Capítulo V, sobre los *datos de las Administraciones públicas y* los *servicios en Red*, distribuido en cuatro secciones (Sección I, en relación con los *datos de las Administraciones públicas* –artículos 50 a 57–; Sección II, para la *utilización de los datos* –artículos 58 a 62–; Sección III, que norma los *servicios en Red* –artículos 63 a 65–, y Sección IV, relativa a las cartas electrónicas –artículo 66–); un Capítulo VI, que trata el *desarrollo, adquisición y reutilización de los sistemas informáticos en las Administraciones públicas* y que se extiende desde el artículo 67 al artículo 70; un Capítulo VII, para las *reglas técnicas* (artículo 71), y un Capítulo VIII, que contiene las *disposiciones transitorias finales y derogaciones* (artículos 72 a 76).

2. El nuevo Reglamento europeo sobre identificación electrónica y servicios de confianza para las transacciones electrónicas y su aplicación en España e Italia

En este nuevo apartado, procede estudiar la repercusión de la nueva normativa europea en materia de identificación electrónica y servicios de confianza, primero de manera individualizada y, después, en su repercusión sobre los sistemas jurídicos de España e Italia. Es por ello que, sobre la base de un nuevo cuadro comparativo sobre las equivalencias de estas tres normativas interrelacionadas (**anexo XV**), examinaremos los aspectos legales más relevantes de cada una de ellas.

Autores como DE MIGUEL ASENSIO[416] explican el contexto que motivó el cambio que ahora nos ocupa, y lo hace en los siguientes términos:

«En pocos sectores la elaboración en el seno de la UE de un complejo marco normativo creado al hilo del desarrollo de la sociedad de la información ha resultado tan poco operativo en la práctica como en el ámbito de las firmas electrónicas. Esa situación es la consecuencia en buena medida de que la orientación y el contenido de la normativa de armonización adoptada mediante la Directiva 1999/93/CE determinaron que los mecanismos de firma electrónica típicamente utilizados en el ámbito del comercio electrónico prácticamente no fueran objeto de atención legislativa, así como que otros posibles mecanismos tecnológicos relevantes para aportar seguridad al comercio electrónico quedaran al margen de ese régimen legal. Asimismo, las dificultades de aplicación o el carácter innecesario de ciertos requisitos legales,

[416] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 126.

la inadecuación de algunas de las limitaciones previstas, o el carácter inviable de ciertos elementos básicos de la Directiva 1999/93/CE y de sus normas de transposición han motivado una profunda transformación en este ámbito en el seno de la UE».

En este contexto, tiene lugar el 28 de agosto de 2014 la publicación del RIE-SCTE[417], que, derogando el texto anterior (artículo 50), instaura un nuevo sistema en materia de identificación electrónica y servicios de confianza. Su entrada en vigor se producirá veinte días después de su publicación; no obstante, las disposiciones en él contenidas experimentarán, como regla general, una aplicación diferida al próximo 1 de julio de 2016, a excepción de una serie de artículos que, contenidos en el apartado segundo del artículo 52 eIDAS, comenzarán a aplicarse en un momento diferente[418]. Hasta dicha fecha, cabía entender no producido el efecto

[417] Varios han sido los estudiosos, nacionales e internacionales, que han realizado una primera e interesante aportación doctrinal sobre este nuevo Reglamento y su influencia a nivel interno de los Estados miembros; entre otros, *vid.* FINOCCHIARO, G. D., «Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari», *Le nuove leggi civili commentate*, vol. 3, 2015, pp. 419 a 428; GÓMEZ LOZANO, M. M., «Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 199», *Ars iuris Salmanticensis: revista europea e iberoamericana de pensamiento y análisis de Derecho, Ciencia, Política y Criminología*, vol. 1, 2015, pp. 267 a 269; GONZÁLEZ ROBLES, A./POHLMANN, N./ENGLING, C. Y OTROS, «Doubtless identification and privacy preserving of user in cloud systems», en POHLMANN, N./REIMER, H./SCHNEIDER, W. (coords.) *Securing electronic business processes*, Berlín, Springer, 2015, pp. 98 a 108; LAFUENTE SUÁREZ, M., «El "nuevo" Reglamento UE 910/2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior, tras un año desde su publicación en el DOUE», *Actualidad jurídica Aranzadi*, vol. 911, 2015, pp. 12 a 18; LEONE, C., «EU Regulation no. 910/2014 on electronic identification and trust services: an effort towards the elimination of barriers for electronic transactions and internal market consolidation», *Rivista italiana di Diritto pubblico comunitario*, vol. 3-4, 2015, pp. 1045 a 1060; LORENTE HOWELL, J. L., «Banca electrónica y Reglamento elDAS», *Actualidad jurídica Aranzadi*, vol. 927, 2017, pp. 1 y 2; MERCHÁN MURILLO, A., *Firma electrónica: funciones y problemática. Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, Cizur Menor, Aranzadi, 2016, pp. 31 a 296; RICO CARRILLO, M., «El Reglamento europeo sobre identificación y servicios de confianza electrónicos», *Revista general de Derecho europeo*, vol. 35, 2015, pp. 2 a 24, o ROJO GIL, F./ALAMILLO DOMINGO, I., «Firma y sello electrónicos: el porqué y el cómo de la implantación del nuevo reglamento europeo», *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, vol. 74, 2016, pp. 28 y 29.

[418] Estas disposiciones son: a) las contenidas en los artículos 8, apartado 3; 9, apartado 5; 12, apartados 2 a 9; 17, apartado 8; 19, apartado 4; 20, apartado 4; 21, apartado 4; 22, apartado 5; 23, apartado 3; 24, apartado 5; 27, apartados 4 y 5; 28, apartado 6; 29, apartado 2; 30, apartados 3 y 4; 31, apartado 3; 32, apartado 3; 33, apartado

derogatorio o de inaplicación pretendido, de modo que tanto la DFE como la LFE resultaban vigentes y plenamente aplicables a todos los efectos[419].

Una de las principales innovaciones que trae consigo el nuevo texto radica en el instrumento jurídico utilizado: la figura del reglamento sustituye ahora a la de la directiva. El artículo 288 TFUE[420], en su párrafo segundo, define el reglamento como norma de alcance general, de carácter obligatorio en todos sus elementos y directamente aplicable en cada uno de los Estados miembros, sin necesidad de acto previo e individual alguno de incorporación. En cambio, de la directiva sostiene, un párrafo después, que obligará al Estado miembro destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios necesarios para alcanzarlo. De este modo, con la adopción del reglamento se persigue uniformizar, en lugar de armonizar (directiva), el Derecho sobre la materia, eliminando aquellas pequeñas diferencias que no harían sino dificultar el objetivo final de interoperabilidad técnico-jurídica para el conjunto de los veintiocho Estados[421].

Se persigue, así, incrementar, a lo largo y ancho del territorio europeo, el nivel de seguridad y de confianza de todos los agentes del mercado (consumidores, empresas y Administraciones Públicas) en el entorno en línea, favoreciendo la progresiva consolidación de un espacio único digital capaz de posibilitar, de un modo verdaderamente eficaz, la realización de

2; 34, apartado 2; 37, apartados 4 y 5; 38, apartado 6; 42, apartado 2; 44, apartado 2; 45, apartado 2, y 47 y 48, que comenzarán a aplicarse a partir del día 17 de septiembre de 2014 –artículo 52.2.a) eIDAS–; b) las contempladas en los artículos 7; 8, apartados 1 y 2; 9; 10; 11, y 12, apartado 1, que se aplicarán a partir de la fecha de aplicación de los actos de ejecución que se hallan previstos en los artículos 8, apartado 3, y 12, apartado 8 –artículo 52.2.b) eIDAS–, y c) la prevista en el artículo 6, que se aplicará a partir de los tres años desde la fecha de aplicación de los actos de ejecución previstos en los artículos 8, apartado 3, y 12, apartado 8 –artículo 52.2.c) eIDAS–.

[419] ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 715.

[420] DOUE C 83, de 30 de marzo de 2010, p. 47.

[421] FINOCCHIARO, G. D., «Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari», cit., p. 422; RICO CARRILLO, M., «El Reglamento europeo sobre identificación y servicios de confianza electrónicos», cit., p. 22.

transacciones por vía electrónica y el desarrollo de nuevos negocios *online*[422]. En concreto, el objetivo perseguido por la nueva normativa no es otro que el de «[…] garantizar el correcto funcionamiento del mercado interior aspirando al mismo tiempo a un nivel de seguridad adecuado de los medios de identificación electrónica y los servicios de confianza», a cuya consecución se encaminan tres acciones concretas: en primer lugar, establecer las condiciones en las que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro; en segundo lugar, crear normas jurídicas para los servicios de confianza, en particular para la realización de transacciones electrónicas, y, en tercer lugar, configurar un marco jurídico para los documentos electrónicos, las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web (artículo 1 RIE-SCTE). En otras palabras, el nuevo texto, si bien mantiene el régimen regulatorio de la firma electrónica, incorpora en su objeto otros mecanismos, también de gran relevancia desde la óptica de la seguridad y de la confianza en el marco del comercio electrónico, como sucede con los sellos electrónicos, los sellos de tiempo electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web[423]; ello responde al hecho de que, frente al modelo anterior encarnado por la Directiva, el Reglamento busca proporcionar un marco global capaz de garantizar unas transacciones electrónicas fiables, y todo ello al tiempo que persigue eliminar los obstáculos existentes para el uso transfronterizo de los medios de identificación electrónica empleados en los Estados miembros como instrumentos de autenticación, al menos en los servicios públicos.

---

[422] LEONE, C., «EU Regulation no. 910/2014 on electronic identification and trust services: an effort towards the elimination of barriers for electronic transactions and internal market consolidation», cit., pp. 1045 y 1046. Inevitable sería plantearse, subsiguientemente, la posible aplicación de estas medidas más allá de las fronteras de la UE, esto es, a nivel internacional; esta cuestión es planteada por numerosos autores, entre los que destacan ALBA, M., «Order out of chaos: technology, intermediation, trust and reliability as the basis for the recognition of legal effects in electronic transactions», *Creighton University law review*, vol. 47, 2014, p. 387; BEAUPÉRIN, T., «Think small first in the EU?: a reality check», *Eurochambres report on the European Commission's application of the SME Test*, vol. 5, 2014, p. 93, o RUGGERI, L., «ADR y ODR y su taxonomía. La identificación de caracteres», *Revista de Internet, Derecho y Política*, vol. 10, 2010, p. 100.

[423] RICO CARRILLO, M., «El Reglamento europeo sobre identificación y servicios de confianza electrónicos», cit., p. 6.

El Reglamento se estructura en un total de cincuenta y dos artículos, que se distribuyen a lo largo de seis capítulos (Capítulo I, sobre *disposiciones generales*, que comprende los cinco primeros artículos; Capítulo II, comprensivo de la *identificación electrónica* como uno de los ejes principales en torno a los cuales pivota la norma, que abarca los artículos 6 a 12; Capítulo III, para los *servicios de confianza*, el otro gran pilar de la actual regulación, dividido, a su vez, en ocho secciones –Sección 1, para las *disposiciones generales*, que contiene los artículos 13 a 16; Sección 2, para la *supervisión* por parte de los organismos de supervisión, que abarca los artículos 17 a 19; Sección 3, para los *servicios de confianza cualificados*, que se extiende desde el artículo 20 al 24; Sección 4, para la *firma electrónica* de personas físicas, SSIisc por excelencia y único existente en la DFE anterior, integrada por los artículos 25 a 34; Sección 5, para los *sellos electrónicos* de personas jurídicas, comprensiva de los artículos 35 a 40; Sección 6, para el *sello de tiempo electrónico*, artículos 41 y 42; Sección 7, para el *servicio de entrega electrónica certificada*, que estará constituida por los artículos 43 y 44, y Sección 8, para el servicio de *autenticación de sitios web*, artículo 45–; Capítulo IV, relativo a los *documentos electrónicos*, integrado por un único precepto 46; Capítulo V, sobre *delegación de poderes y disposiciones de ejecución*, que abarcará los artículos 47 y 48, y un último Capítulo VI, que concluye con las *disposiciones finales*, a lo largo de los artículos 49 a 52.

Con posterioridad a su publicación, se han publicado dos correcciones de errores al Reglamento por parte del Parlamento Europeo y del Consejo: una primera, de 1 de noviembre de 2016[424], y una segunda, de 20 de abril de 2017[425].

También, y fruto de la labor de desarrollo encomendada a la Comisión, ha tenido lugar la promulgación de una serie de actos de ejecución que persiguen complementar el Reglamento en aspectos concretos; estos son, por orden cronológico, los siguientes: DEMPCEMMIE[426];

[424] DOUE L 296, de 1 de noviembre de 2016, p. 25.

[425] DOUE L 104, de 20 de abril de 2017, p. 28.

[426] DOUE L 53, de 25 de febrero de 2015, p. 14.

REERFECUESCC[427]; REFEPTMNSMIE[428]; REMI[429]; DEETFLC[430]; DEEFFEASEA[431]; DECFPN[432] y DENESDCCFS[433].

## 2.1. Normativa española reguladora de determinados aspectos de los servicios electrónicos de confianza

Como efecto más inmediato, la entrada en vigor del RIE-SCTE ha provocado en nuestro país el desplazamiento intrínseco de la LFE en todo aquello regulado por el Reglamento, haciendo necesaria la inmediata adaptación o derogación definitiva de una norma que, como sabemos (y pese a cuanto se diga en su Exposición de Motivos), nació para incorporar la (ya derogada) DFE al ordenamiento jurídico español. En este contexto, y en aras de una mayor certeza y seguridad jurídica, tiene lugar el pasado 4 de abril de 2017 una propuesta legislativa que persigue sustituir la normativa anterior en materia de firma electrónica por una nueva ley que se ajuste a la incipiente regulación comunitaria, «[…] eliminando los preceptos incompatibles con el Reglamento para evitar la apariencia jurídica de su vigencia y aplicabilidad, así como regulando determinados aspectos de los servicios electrónicos de confianza que el Reglamento deja al criterio de los Estados miembros»[434].

---

[427] DOUE L 128, de 23 de mayo de 2015, p. 13.

[428] DOUE L 235, de 9 de septiembre de 2015, p. 7.

[429] DOUE L 235, de 9 de septiembre de 2015, p. 1. Posteriormente, se ha publicado una corrección de errores a este Reglamento (DOUE L 28, de 4 de febrero de 2016, p. 18).

[430] DOUE L 235, de 9 de septiembre de 2015, p. 26. De conformidad con este Reglamento, se ha publicado la Información 2016/C 233/01 relativa a los datos sobre las listas de confianza de los Estados miembros notificada en virtud de la Decisión 2009/767/CE, modificada por la Decisión 2010/425/UE y la Decisión de ejecución 2013/662/UE, y en virtud de la Decisión de ejecución (UE) 2015/1505 (DOUE C 233, de 28 de junio de 2016, p. 1). También, posteriormente, se ha publicado una corrección de errores a este Reglamento (DOUE L 59, de 7 de marzo de 2017, p. 41).

[431] DOUE L 235, de 9 de septiembre de 2015, p. 37.

[432] DOUE L 289, de 5 de noviembre de 2015, p. 18.

[433] DOUE L 109, de 26 de abril de 2016, p. 40.

[434] Memoria del análisis de impacto normativo del Anteproyecto de Ley reguladora de determinados aspectos de los servicios electrónicos de confianza.

Surge de este modo lo que conocemos como ALSEC, que, habiendo recabado el informe preceptivo de la Secretaría General Técnica del Ministerio de Energía, Turismo y Agenda Digital, conforma un articulado que afecta a los PSSIisc, complementando el RIE-SCTE (artículo 1) en relación con las obligaciones a las que estos están sometidos y las condiciones necesarias para la prestación de este tipo de servicios en el mercado nacional, promoviendo, en definitiva, la competencia sobre las bases de unas reglas comunes. Con ello pretende, ante todo, eliminar el riesgo de situaciones de inseguridad jurídica en las relaciones telemáticas a efectuar con ciudadanos, empresas y Administraciones Públicas, motivadas por la transición al nuevo marco legislativo comunitario, que traen consigo diferencias de interpretación de las normas aplicables. Además, se evitan los vacíos normativos que hubiera provocado el mantenimiento de la LFE a los SSIisc distintos de la firma electrónica y regulados por primera vez con el Reglamento, en especial, en lo que respecta al régimen sancionador, que no puede ser objeto de aplicación analógica a éstos. Por último, se regulan aquellos aspectos que el RIE-SCTE remite a los sistemas nacionales de cada Estado miembro, como sucede, entre otros, con los efectos legales de algunos SSIisc cualificados, con el régimen de responsabilidad y de previsión de riesgo de los PSSIisc, con la comprobación de la identidad y los atributos de los solicitantes de un certificado cualificado, con la inclusión de requisitos adicionales a nivel nacional para certificados cualificados (tal es el caso de los identificadores nacionales o el tiempo máximo de vigencia), o, en fin, con el régimen de suspensión de certificados.

Este Anteproyecto vendrá precedido de una consulta pública, contemplada en el artículo 26.2 LG[435], sobre la adaptación del ordenamiento jurídico español al RIE-SCTE, presentada el 21 de noviembre de 2016 por el Ministerio de Energía, Turismo y Agenda Digita, así como de una ronda de entrevistas con el sector de los PSSIisc y con los principales usuarios, incluyendo a las Administraciones públicas. En dicha consulta se plantearán, en términos generales, aspectos varios, como los problemas a solucionar por el nuevo texto, la necesidad y oportunidad de su aprobación, los objetivos a perseguir, las posibles soluciones alternativas de adaptación legal y el contenido de la consulta propiamente dicha; en él se abordarán aspectos legales no regulados por el Reglamento (como la comprobación de la identidad y atributos de los solicitantes de un certificado electrónico cualificado, los requisitos a nivel nacional para dichos certificados, el mantenimiento por parte de los PSSIisc cualificados de

[435] BOE núm. 285, de 28 de noviembre de 1997.

recursos financieros suficientes u obtención de pólizas de seguros de responsabilidad adecuadas para hacer frente a una posible responsabilidad por daños y perjuicios, el régimen sancionador o el mantenimiento de un servicio de información en la página web de este Ministerio sobre los PSSIisc no cualificados), la regulación de nuevos SSIisc a nivel nacional al amparo del considerando 25 del Reglamento eIDAS, el desarrollo de lo establecido en el artículo 25 LSSICE o cualquier otra cuestión en la que se desee incidir. Fruto de esta consulta pública tendrá lugar, posteriormente, la emisión de un documento por parte del Ministerio de Energía, Turismo y Agenda Digital sobre valoración de las respuestas recibidas; también de una Memoria del análisis de impacto normativo del Anteproyecto.

Por lo demás, el ALSEC consta de cinco títulos: el Título I (artículos 1 a 3), intitulado *disposiciones generales*, contiene los principios generales que delimitan los ámbitos, subjetivo y objetivo, de aplicación del Anteproyecto, así como los efectos jurídicos de los documentos electrónicos; el Título II (artículos 4 a 9), por su parte, regula el régimen aplicable a los *certificados electrónicos*, incluyendo el DNIe; el Título III (artículos 10 a 16) recoge las *obligaciones y* régimen de *responsabilidad de los prestadores de servicios electrónicos de confianza*, ya sean cualificados o no cualificados; el Título IV (artículos 17 a 20) dedica su contenido a disciplinar el régimen de supervisión y control de los PSSIisc, y, por último, el Título V (artículos 21 a 23) regula las *infracciones* (muy graves, graves y leves) a la norma, que conllevarán la imposición de las correspondientes *sanciones*. Cierra el texto un total de dos D.A. (la primera sobre *fe pública y servicios electrónicos de confianza*, la segunda para los *efectos jurídicos de los sistemas utilizados en las Administraciones públicas*), una D. T. Única (que contempla un aspecto clave, como es la *comunicación de actividad por prestadores de servicios no cualificados ya existentes* antes de la entrada en vigor de la futura Ley), una D. D. Única (sobre *derogación normativa*, que prevé la supresión de la LFE, del artículo 25 LSSICE[436] y de la ORAPSSIisc) y dos D. F. (la primera para la *modificación de la Ley 56/2007, de 28 de diciembre, de medidas de impulso de la sociedad de la información* y la segunda para el *fundamento constitucional*).

[436] Y es que, como indica en el apartado V de su Exposición de Motivos, estos SSIi se encuentran subsumidos en los tipos regulados por el RIE-SCTE, fundamentalmente en los servicios de entrega electrónica certificada –artículos 3.36) y 37), 43 y 44–, que incluyen el archivado de las evidencias correspondientes.

### 2.2. Adaptación legislativa italiana a la reciente modificación normativa comunitaria

En Italia, el efecto de la reforma legislativa europea se ha traducido en la profunda adaptación que del CAD ha llevado a cabo la SDLMICAD[437]. En lo que aquí nos interesa, esta transformación plasma la necesidad, ya desde antes evidenciada, de garantizar el derecho de acceso a los datos, a los documentos y a los servicios relacionados con ellos de forma virtual, simplificando las modalidades de acceso a tales servicios y conformando las bases para una auténtica *ciudadanía digital*.

Más específicamente, la norma, con un total de sesenta y seis artículos, plasma la necesidad de adecuar el Reglamento comunitario al ordenamiento jurídico nacional, armonizando las condiciones para el reconocimiento recíproco en el ámbito de la identificación electrónica, y creando, al mismo tiempo, unas reglas comunes para el conjunto de SSIisc recogidos en el RIE-SCTE. Ello exige, en primer lugar, la adopción por el SDLMICAD de todas las definiciones contenidas en el Reglamento europeo, amén de la consiguiente derogación de muchas otras contenidas originariamente en el CAD; en cualquier caso, permanece la definición de *firma digital*, creación propia del sistema italiano. A todo ello se añade, como aspectos también relevantes, la ampliación del ámbito de aplicación subjetivo y objetivo del CAD y el establecimiento de importantes sanciones a cargo de los PSSIisc cualificados, de los gestores de correo electrónico certificado, de los gestores de la identidad digital y de los conservadores, en caso de incumplimiento de la norma.

[437] Gazzetta Ufficiale num. 214, 13 settembre 2016. En torno a esta cuestión, *vid.* LEONE, C., «EU Regulation no. 910/2014 on electronic identification and trust services: an effort towards the elimination of barriers for electronic transactions and internal market consolidation», cit., pp. 1053 a 1060.

# CAPÍTULO TERCERO
# FIRMA ELECTRÓNICA COMO MEDIO DE PRUEBA DE CONTRATOS ELECTRÓNICOS DE NATURALEZA PRIVADA

**SUMARIO**. - **I.** SERVICIOS ELECTRÓNICOS DE CONFIANZA. **1.** Naturaleza intermediadora. **2.** Equivalencia internacional. **II.** FIRMA ELECTRÓNICA: ASPECTOS GENERALES. **1.** Sistemas alternativos de cifrado criptográfico. **1.1.** Criptografía simétrica. **1.2.** Criptografía asimétrica: especial atención a la firma digital. **2.** Certificados de firma electrónica. **2.1.** Certificados electrónicos cualificados. **2.2.** Vigencia, suspensión y extinción. **3.** Datos y dispositivos de firma electrónica. **3.1.** Datos y dispositivos de creación. **3.2.** Datos y dispositivos de verificación o validación. **4.** Concepto y clases de firma electrónica. **4.1.** Firma electrónica general *versus* firma electrónica simple. **4.2.** Firma electrónica avanzada. **4.3.** Firma electrónica cualificada. **III.** EFECTOS LEGALES DE LA FIRMA ELECTRÓNICA. **1.** Aspectos materiales. **1.1.** Firma electrónica cualificada: equivalencia funcional con la firma manuscrita y equiparación a nivel comunitario. **1.2.** Firmas electrónicas no cualificadas. **1.3.** Reconocimiento de la autonomía de la voluntad de las partes. **2.** Aspectos procesales. **2.1.** Documento electrónico: el problema de la antinomia legislativa en materia de prueba. **2.2.** Solicitud de eficacia o impugnación de un contrato acompañado de firma electrónica. **2.3.** Aportación al proceso de contratos electrónicos de naturaleza privada.

## I. SERVICIOS ELECTRÓNICOS DE CONFIANZA

El presente capítulo parte de un importante concepto, quizás uno de los más relevantes a la hora de explicar el funcionamiento de la nueva normativa comunitaria y, con ello, de la firma electrónica como instrumento esencial para generar confianza suficiente en el empleo del comercio electrónico; hablamos de los SSIisc. En las siguientes líneas, procuraremos arrojar algo de luz en torno a la naturaleza peculiar de estos servicios y a la ampliación que con el RIE-SCTE tiene lugar, al prever su posible equivalencia jurídica más allá de las fronteras propias de la UE.

## 1. Naturaleza intermediadora

Como decíamos, dentro del nuevo Reglamento europeo eIDAS presenta singular importancia el concepto de *servicios de confianza* (SSIisc), que, como tendremos ocasión de analizar con más detalle en el último capítulo de este estudio, serán prestados por los denominados *prestadores de servicios de confianza* (PSSIisc). De acuerdo con el artículo 3.16) de la norma, un SSIisc puede ser definido[438] como:

> «[E]l servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en[439]:
>
> a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o
>
> b) la creación, verificación y validación de certificados para la autenticación de sitios web, o
>
> c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios»[440].

[438] Cierto es, como señalan ALMONACID LAMELAS, V./ALAMILLO DOMINGO, I., «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», en CAMPOS ACUÑA, M. C. (coord.) *El nuevo procedimiento administrativo local tras la Ley 39/2015*, Las Rozas, Wolters Kluwer, 2016, p. 428, que, más que una definición, se trata de una enumeración. Estos autores sí que aportan, no obstante, una conceptualización de SSIisc como «[…] aquellas tecnologías en las que se puede confiar, por lo que modifican la percepción del usuario con respecto a la vulnerabilidad de un proceso al que se incorporan. Para ello, el usuario debe poder reconocer un servicio de confianza, de hecho, como suficientemente confiable» (*Ibid.*, p. 429).

[439] Lista cerrada, al objeto de delimitar el alcance de la regulación uniforme europea. No obstante, los Estados conservan la libertad para definir otros tipos de SSIisc a efectos de su reconocimiento a nivel nacional como SSIisc cualificados, así como mantener o introducir disposiciones nacionales, acordes con el Derecho de la Unión, relativas a los SSIisc, «[…] siempre que tales servicios no estén plenamente armonizados en el presente Reglamento» (considerandos 24 y 25 Reglamento eIDAS).

[440] Artículo 34 RIE-SCTE, que limita el SSIisc cualificado de conservación de firmas electrónicas cualificadas al PSSIisc cualificado «[…] que utilice procedimientos y tecnologías capaces de ampliar la fiabilidad de los datos de la firma electrónica cualificada más allá del período de validez tecnológico». En todo caso, habilita a la Comisión para, mediante actos de ejecución a adoptar con arreglo al procedimiento de examen contemplado en el artículo 48.2, establecer números de referencia de normas relativas al SSIisc cualificado de conservación de firmas electrónicas cualificadas, presumiéndose el cumplimiento de los requisitos antes mencionados cuando

A su vez, indica el apartado siguiente de este mismo precepto, tendrán la consideración de SSIisc *cualificados* aquellos que cumplan los requisitos aplicables establecidos en el Reglamento, siendo prestados por PSSIisc, por ende, *cualificados*. Estos SSIisc cualificados se verán dotados de efectos jurídicos que, al menos supuestamente, los sitúan en una superioridad jurídica respecto de los que no lo son, y lo harán desde tres perspectivas distintas[441]: en primer lugar, ofreciendo una mayor seguridad jurídica de que el medio empleado es idóneo para cumplir con una norma de carácter imperativo, intangible para las partes, que exija firma manuscrita; en segundo lugar, eliminando la necesidad de establecer reglas contractuales o administrativas para concretar los efectos sustantivos de la firma electrónica, y, en tercer y último lugar, favoreciendo la consecución de efectos procesales favorables, habida cuenta de la imposibilidad de que las partes creen nuevos medios de prueba.

Más allá de lo anterior, de un análisis pormenorizado de la estructura de los SSIisc podemos inferir una importante conclusión, como es que forman parte del más amplio concepto, ya estudiado en el primer capítulo, de *servicios de la sociedad de la información*[442]; en concreto, se

los mecanismos de este SSIisc se ajusten a dichas normas. Por lo demás, como bien expone ALAMILLO DOMINGO, I., «Los servicios de confianza y la prueba electrónica», en OLIVA LEÓN, R./VALERO BARCELÓ, S. (coords.) *La prueba electrónica: validez y eficacia procesal*, Juristas con futuro, 2016, pp. 145 y 146, «[…] la denominación **servicios de confianza** contenida en el Reglamento eIDAS constituye una evolución y, al tiempo, **ampliación semántica** sobre la denominación de **servicio de certificación**, y se fundamenta en el hecho de que estos servicios permiten aportar confianza a los procesos de negocio en los que se emplean, en gran medida gracias a los efectos jurídicos que se asocian a dichos servicios. Muestra de ello es que la exposición de motivos del **Reglamento eIDAS** manifieste que *el presente Reglamento se propone reforzar la confianza en las transacciones electrónicas en el mercado interior proporcionando una base común para lograr interacciones electrónicas seguras entre los ciudadanos, las empresas y las administraciones públicas e incrementando, en consecuencia, la eficacia de los servicios en línea públicos y privados, los negocios electrónicos y el comercio electrónico en la Unión* (Considerando (2) del Reglamento eIDAS), para lo cual se precisa ir más allá de la regulación de firma electrónica, la cual no ofrecía "un marco global transfronterizo e intersectorial para garantizar unas transacciones electrónicas seguras, fiables y de fácil uso" (Considerando (3) del Reglamento eIDAS)». Pese a ello, añade, la creación de un nivel reforzado de confianza en estos servicios no proviene de sus propias características técnicas, sino del hecho de que se encuentran regulados.

[441] ALMONACID LAMELAS, V. Y OTROS, «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», cit., pp. 432 y 433.

[442] Conclusión también alcanzada por autores como RICO CARRILLO, M., «El Reglamento europeo sobre identificación y servicios de confianza electrónicos», cit., p. 24.

encuadran dentro de los conocidos como servicios de la sociedad de la información *de intermediación*. La razón estriba en que estos servicios participan por completo de los rasgos que definen a los SSI, que, recordemos, a la luz de lo dispuesto en el artículo 2.a) DCE y en el anexo a) LSSICE, se caracterizan por ser prestados normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del DSSI, comprendiendo también aquellos que, no siendo remunerados por estos últimos, constituyen una actividad económica para el PSSI; a su vez, añadía el apartado b) de este mismo anexo, serán de intermediación (es decir, SSIi) aquellos SSI por los que «[…] se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información». Si analizamos la naturaleza de los SSIisc contenidos en el Reglamento eIDAS podemos ver que, con el objeto de facilitar la prestación o utilización de otros SSI (función intermediadora), son prestados habitualmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual del DSSIisc; de este modo, junto a los SSIi comprendidos en los artículos 12 a 14 DCE y 14 a 17 LSSICE (provisión de servicios de acceso a Internet; transmisión de datos por redes de telecomunicaciones; realización de copia temporal de las páginas de Internet solicitadas por los usuarios; alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros, y provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet), los SSIisc recogidos en el artículos 3.16) y 17) y 13 a 45 RIE-SCTE cierran o, cuanto menos, delimitan en mayor medida el círculo de SSIi aplicables dentro del ordenamiento jurídico español (**anexo XVI**).

Por esta misma razón, entendemos inadecuada la clasificación realizada por autores como MÁRQUEZ LOBILLO[443], quien sostiene que existen tres tipos autónomos de SSI, a saber:

[443] MÁRQUEZ LOBILLO, P., *Empresarios y profesionales en la sociedad de la información*, Madrid, Edersa, 2004, p. 195; MÁRQUEZ LOBILLO, P., «Prestadores de servicios de intermediación: algunas especialidades de su estatuto jurídico», *Revista de la contratación electrónica*, vol. 88, 2007, p. 5. Expresados en términos similares, comparten esta clasificación, entre otros, CAVANILLAS MÚGICA, S./JULIÀ BARCELÓ, R., «La responsabilidad civil por daños causados a través de Internet», en SALA ARQUER, J. M./MARTÍNEZ-SIMANCAS SÁNCHEZ, J. (coords.) *Derecho sobre Internet*, Madrid, Banco Santander Central Hispano, 2008, p. 270; GARCÍA DEL POYO, R./MARTÍNEZ ROJAS, S., «La responsabilidad de los intermediarios», en PÉREZ BES, F. (coord.) *El Derecho de Internet*, Barcelona, Atelier, 2016, pp. 227 y 228; MARTÍN REYES, M. Á., «Los servicios de la sociedd de la información: ámbito coordinado y sujetos de los mismos», *Revista de la contratación electrónica*, vol. 41, 2003, p. 8; PLAZA PENADÉS, J., «La responsabilidad civil en Internet: su regulación en el Derecho comunitario y su previsible incorporación al Derecho español», cit., p. 2171; PLAZA PENADÉS, J., «Breve comentario a la Ley 34/2002, de servicios de la sociedad de la información y comercio electrónico», *Alfa-Redi*, vol. 107, 11 a 52, 2002, p. 14; SÁNCHEZ DEL

en primer lugar, los SSI en sentido estricto; en segundo lugar, y dentro de los anteriores, los SSIi, y, por último, los SSIic. Y es que, por cuanto se ha expuesto, parece más adecuado considerar una única categoría, la de los SSI, de la que se desprende, como modalidad específica, la de los SSIi, uno de los cuales vendrá representado por los SSIisc (antes, SSIic).

En el caso concreto que nos ocupa, como es el análisis de los efectos que conlleva la plasmación de firma en contratos de naturaleza electrónica a la luz de la nueva normativa comunitaria protagonizada por el RIE-SCTE y por los actos conexos dictados a su amparo, podemos concluir que el SSI vendría representado por la contratación electrónica de bienes y servicios –punto 1.º del apartado a) del anexo LSSICE–; a su vez, los concretos SSIi que facilitan su prestación, amén de cuantos puedan existir al amparo de los artículos 12 a 14 DCE y 14 a 17 LSSICE (por ejemplo, la provisión de acceso a Internet para constituir una página web a través de la cual celebrar contratos electrónicos o la transmisión misma de datos relativos a dicho contrato por redes de telecomunicaciones, por no mencionar la realización de copia temporal de la página web solicitada por el usuario –DSSIi y, a su vez, PSSI– o el alojamiento de la página web en los propios servidores de datos), serían aquellos relativos a la creación, verificación, validación y preservación de firmas electrónicas, así como de sus correspondientes certificados, que tendrán la naturaleza de SSIisc y que serán prestados por PSSIisc y recibidos por DSSIisc.

De igual modo, una de las partes del contrato electrónico, más específicamente la persona física (no jurídica, que, con la regulación actual, tendría que emplear otro SSIisc, el sello electrónico) que proporcione el SSI, o, lo que es lo mismo, el bien o servicio objeto del contrato electrónico, tendrá la consideración de PSSI –artículo 2, apartados b) y c), DCE y apartado c) del anexo LSSICE– y será uno de los firmantes del contrato electrónico (aspecto que le atribuye la consideración simultánea de DSSIisc en sus relaciones con el PSSIisc). En cambio, la contraparte, es decir, la persona física que utilice, sea o no por motivos profesionales, este SSI, será el DSSI –artículo, 2, apartados d) y e), DCE y apartado d) del anexo LSSICE–; en

---

CASTILLO, V., «Los servicios de la sociedad de la información, la convergencia de las telecomunicaciones y los servicios de la sociedad de la información en la Ley 34/2002 sobre el comercio electrónico», *Revista de la contratación electrónica*, vol. 73, 2006, p. 53; VATTIER FUENZALIDA, C., «Responsabilidad contractual y extracontractual en el comercio electrónico», cit., pp. 75 y 76; VILLAR URIBARRI, J. M., «El régimen jurídico de los prestadores de servicios de la sociedad de la información», en AA.VV. (coord.) *Derecho de Internet: la Ley de servicios de la sociedad de la información y de comercio electrónico*, Cizur Menor, Aranzadi, p. 395.

este último caso, en su condición de cosignatario del contrato electrónico, el DSSI será también, respecto del PSSIisc, DSSIisc (**anexo XVII**).

2. Equivalencia internacional

Dado el ámbito internacional en el que, con frecuencia, se desenvuelven los SSI, no resultaría operativo que los SSIisc cualificados perdieran su eficacia fuera del territorio de la UE. Es por ello que, con base en el principio de reciprocidad, el artículo 14 RIE-SCTE establece que los SSIisc prestados por PSSIisc establecidos en un tercer país serán reconocidos como legalmente equivalentes a los SSIisc cualificados prestados por PSSIisc cualificados establecidos en la UE si los SSIisc originarios del tercer país son reconocidos en virtud de un acuerdo celebrado entre la UE y el tercer país u organización internacional en cuestión, de conformidad con el artículo 218 TFUE. Estos acuerdos, prosigue el precepto, garantizarán, en particular, dos aspectos básicos: a) que los PSSIisc de terceros países u organizaciones internacionales con los que se celebren acuerdos y los SSIisc que presten cumplen los requisitos aplicables a los PSSIisc cualificados establecidos en la UE y a los SSIisc cualificados que prestan, y b) que los SSIisc cualificados prestados por PSSIisc establecidos en la UE son reconocidos legalmente como equivalentes a los SSIisc prestados por PSSIisc que se hallen establecidos en terceros países u organizaciones internacionales con los que se celebren acuerdos.

Este artículo encuentra su reflejo previo en el artículo 7 DFE[444] que incurría en el error (superado con el RIE-SCTE) de limitar esta equivalencia internacional sólo a los certificados electrónicos, cuando, como bien indicaba su artículo 2.11, los PSSIic podían realizar (una, otra o las dos) tanto la actividad de expedición de certificados electrónicos ($SSIic_1$) como la de prestación de otros servicios en relación con la firma electrónica ($SSIic_2$). Por lo demás, establecía este artículo la obligación de los Estados miembros de velar por que los certificados electrónicos expedidos al público como certificados electrónicos *reconocidos* (término, este último, equivalente al actual de *cualificados*) por parte de un PSSIic establecido en un tercer país, fueran reconocidos como jurídicamente equivalentes a los expedidos por un PSSIic establecido en la UE, siempre y cuando se satisficieran algunas de las siguientes tres condiciones: a) que el PSSIic establecido en el Estado no comunitario cumpliera los requisitos establecidos en la DFE y hubiera sido acreditado en el marco de un sistema voluntario de

[444] Ver también considerando 23 DFE.

acreditación (artículo 3.2 DFE) establecido en un Estado miembro; b) que un PSSIic establecido en la UE que cumpliera las prescripciones de la DFE avalase el certificado electrónico expedido por un PSSIic establecido en un Estado no comunitario, o c) que el PSSIic establecido en un Estado no miembro o el certificado electrónico por él expedido fuesen reconocidos en virtud de un acuerdo bilateral o multilateral con la UE[445].

En el mismo defecto anterior incurrirán en nuestro país tanto el artículo 10 RDLFE, primero, como el artículo 14 LFE, después; de acuerdo con este último precepto, los certificados electrónicos (no también, en su caso, otros servicios en relación con la firma electrónica) que los PSSIic establecidos en un Estado que no fuera miembro del EEE[446] expidan al público como certificados electrónico reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los PSSIic establecidos en España, siempre que se cumplan cualquiera de las siguientes exigencias: a) que el PSSIic establecido en el Estado no miembro del EEE reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados electrónicos reconocidos y haya sido certificado conforme a un sistema voluntario de certificación (artículo 26 LFE) establecido en un Estado miembro del EEE; b) que el certificado electrónico expedido por un PSSIic establecido fuera del EEE esté garantizado por un PSSIic establecido dentro del EEE que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos, o c) que el PSSIic establecido

[445] Sobre esta cuestión, *vid.* DE MIGUEL ASENSIO, P. A., «Regulación de la firma electrónica: balance y perspectivas», *Direito da sociedade da informaçao*, vol. 5, 2004, pp. 28 a 30.

[446] Hasta el proceso de separación del Reino Unido de la UE, los Estados que integraban la UE eran: Alemania (1958), Austria (1995), Bélgica (1958), Bulgaria (2007), Chipre (2004), Croacia (2013), Dinamarca (1973), Eslovaquia (2004), Eslovenia (2004), España (1986), Estonia (2004), Finlandia (1995), Francia (1958), Grecia (1981), Hungría (2004), Irlanda (1973), Italia (1958), Letonia (2004), Lituania (2004), Luxemburgo (1958), Malta (2004), Países Bajos (1952), Polonia (2004), Portugal (1986), Reino Unido (1973), República Checa (2004), Rumanía (2007) y Suecia (1995); por su parte, conformaban el EEE los Estados de la UE más más Islandia, Liechtenstein y Noruega. De este modo, con la redacción del artículo 14, la LFE ampliaba el ámbito de aplicación de la equivalencia internacional a estos tres últimos Estados.

fuera del EEE o el certificado electrónico por él expedido estén reconocidos en virtud de un acuerdo bilateral o multilateral con la UE[447].

Como podemos observar, la DFE (y, con ella, el RDLFE y la LFE) configuraba esta equivalencia internacional desde una perspectiva fundamentalmente unilateral, previendo, en esencia, los requisitos que habrán de satisfacer los certificados electrónicos reconocidos de terceros países que quieran operar dentro de las fronteras de la UE. Sin embargo, el RIE-SCTE, persiguiendo el mismo objetivo de reconocimiento mundial, lo hace desde una óptica recíproca e integral; en efecto, con los acuerdos así celebrados, el nuevo Reglamento busca una auténtica eficacia global, no sólo de los SSIisc de terceros países u organizaciones internacionales dentro del ámbito comunitario, sino también de los SSIisc cualificados existentes dentro del territorio de la UE en la demarcación de aquellos. Y lo busca, bien es cierto, de una manera un tanto más laxa o con requisitos, cuanto menos, no tan exigentes como su predecesora, ya que no requerirá que el PSSIisc del tercer país cumpla las exigencias contempladas en el RIE-SCTE, como tampoco exigirá que un PSSIisc establecido en la UE que cumpla las prescripciones del Reglamente avale el SSIisc del Estado no comunitario.

## II. FIRMA ELECTRÓNICA: ASPECTOS GENERALES

Uno de los más laudables efectos propiciados por la nueva sociedad de la información consiste en el intercambio de datos de todo tipo entre los distintos sujetos que la integran. Estas comunicaciones o transferencias electrónicas de información pueden producirse en el ámbito del sector público (entre las distintas Administraciones públicas –A2A– y entre estas con empresarios –A2B/B2A– o con administrados –A2C/C2A–) o en el del sector privado (relaciones entre empresas –B2B–, entre empresarios y consumidores –B2C/C2B– o entre estos –C2C–), y tanto a nivel internacional como puramente interno. Sin embargo, la ampliación por la electrónica de los formatos en que se pueden contener los documentos constitutivos de relaciones negociales o administrativas conlleva también, como no podía ser de otra

[447] Quizás hubiera sido más adecuado establecer dentro de los posibles Estados suscriptores del acuerdo a aquellos que, no perteneciendo a la Comunidad Europea, sí que forman parte del EEE, ya que es este el espacio territorial tenido en cuenta en todo momento a la hora de redactar el precepto.

manera, la aparición de riesgos e incertidumbres, que se ven incrementados cuando las transacciones se efectúan (algo habitual) a través de la Red de redes, Internet[448].

Pues bien, de entre todos estos potenciales inconvenientes, el presente trabajo persigue ofrecer una aproximación teórico-jurídica a aquellos que surgen como consecuencia del intercambio de bienes y servicios en el nuevo comercio virtual, más concretamente en el contexto de la celebración de contratos por vía electrónica. En estos casos, dadas las inseguridades inherentes al sistema, resulta adecuado garantizar una serie de efectos que permitan inferir la confianza suficiente en quienes participen de la transacción[449]: en primer lugar, que el mensaje de datos provenga de quien dice ser (identificación autenticada); en segundo lugar, que dicho mensaje no se haya visto alterado durante el tránsito que va desde que se envía hasta que se recibe (integridad); en tercer lugar, que ni la persona que lo envía pueda negar haberlo enviado ni la persona que lo recibe pueda negar haberlo recibido (no repudio en origen y no repudio en destino, respectivamente), y, en cuarto y último lugar, que su contenido no pueda ser conocido por terceros no autorizados (confidencialidad).

La firma electrónica se erige como la manifestación por antonomasia del importante principio de equivalencia funcional propio del Derecho de la contratación electrónica[450] y como la solución técnica más adecuada para probar la existencia de los extremos arriba suscritos.

---

[448] MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», cit., p. 218.

[449] BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 408; PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», cit., pp. 491 y 492; SANJURJO REBOLLO, B., *Lexnet abogados: notificaciones electrónicas y presentación de escritos y demandas*, Madrid, Dykinson, 2016, pp. 68 y 69; VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., pp. 41 a 44.

[450] Como indica ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, Cizur Menor, Aranzadi, 2008, p. 36, la firma electrónica persigue el cumplimiento de los mismos fines que la firma manuscrita, si bien con un mayor grado de seguridad y de fiabilidad; en la misma línea, FERNÁNDEZ DOMINGO, J. I., «La contratación electrónica y el Real Decreto-ley 14/1999 sobre firma electrónica», cit., pp. 527 a 548; JULIÀ BARCELÓ, R., *Comercio electrónico entre empresarios: la formación y prueba del contrato electrónico (EDI)*, cit., p. 209; SEGURA DE LASSALETA, R., «La seguridad de la contratación en Internet: la firma electrónica», *Revista general de Derecho*, vol. 670, 2000, pp. 8999 a 9012; VATTIER FUENZALIDA, C., «El régimen legal de la firma electrónica», *Actualidad civil*, vol. 1, 2000, pp. 411 a 419.

A continuación, analizaremos cada uno de los elementos que conforman la firma electrónica en sus distintas modalidades, a fin de aproximarnos más adecuadamente a esta figura.

1. Sistemas alternativos de cifrado criptográfico

El empleo efectivo de las posibilidades de comunicación que ofrece actualmente Internet exige la presencia de mecanismos que permitan acreditar la identidad del transmitente o comprobar el origen y la integridad de los datos comunicados. En este sentido, un instrumento esencial que permite dotar de seguridad a la transmisión y al almacenamiento de los datos relativos a los contratos electrónicos que circulan a través de las redes informáticas es la criptografía. *Cifrar* (o su equivalente anglosajón *encriptar*) alude al proceso en virtud del cual la información deviene ininteligible, a fin de protegerla frente a terceros de su modificación y acceso no autorizado, pudiendo volver en cualquier momento al estado anterior a través de un proceso de *descifrado*, todo ello mediante la aplicación de los algoritmos necesarios por parte de quien se encuentre en posesión de la clave adecuada[451]. Más específicamente, el sistema criptográfico es un sistema de tratamiento de la información que transforma el mensaje, de modo que sólo las personas en posesión de algoritmos (procedimiento matemático) y claves (conjunto de dígitos alfanuméricos) adecuados pueden acceder a su contenido de manera correcta y satisfactoria[452].

---

[451] RIBAGORDA GARNACHO, A., «Seguridad informática», en ILLESCAS ORTIZ, R./RAMOS HERRANZ, I. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, p. 18. Según la RAE, se entiende por tal el proceso de «[t]ranscribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger». Así pues, la criptografía es el arte de ocultar lo escrito, en una suerte de proceso conocido como *encriptación*, *cifrado* o *codificación*; a su vez, y en un afán por analizar los mensajes ocultos, nace el *criptoanálisis* (GONZÁLEZ NAVARRO, F., «Comentario al art. 45 de la Ley de régimen jurídico de las Administraciones públicas y procedimiento administrativo común», cit., p. 28). A la suma de las dos disciplinas anteriores se le denomina *criptología*.

[452] GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, cit., p. 57. Para un estudio más profundo acerca de la evolución experimentada por la criptografía a lo largo del tiempo, *vid.* ADIEGO RODRÍGUEZ, J., «Problemática informática de la protección de obras digitales protegidas», en MATA Y MARÍN, R. M./JAVATO MARTÍN, A. M. (coords.) *La propiedad intelectual en la era digital: límites e infracciones a los derechos de autor en Internet*, Las Rozas, La Ley, 2011, pp. 25 y 26; FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., pp. 81 a 114; MARTONI, M., *Firme elettroniche: profili informatico-giuridici*, cit., p. 17. Para un análisis de las aplicaciones y políticas de cifrado, *vid.* DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 110 a 113. Sobre el cifrado como instrumento de confidencialidad en las comunicaciones electrónicas, *vid.* GONZÁLEZ DE LA GARZA, L. M., *Comunicación pública en Internet*, Madrid,

Cuando es bilateral y electrónica, la información contenida en un mensaje de datos es cifrada por el emisor con el objetivo de que su contenido sólo pueda ser conocido por quien resulte ser el receptor pretendido, existiendo, a tales efectos, dos escenarios ciertamente diferentes: un primer escenario, en el que la misma clave es conocida por ambas partes (criptografía simétrica), y un segundo, en el que cada clave es conocida sólo por la parte que la posee (criptografía asimétrica)[453].

### 1.1. Criptografía simétrica

La *criptografía simétrica*, *de clave compartida*, *de clave secreta* o *de una sola clave*, es aquella en la que la clave de cifrado utilizada por el emisor en origen y la clave de descifrado empleada por el receptor en destino para encriptar y desencriptar, respectivamente, el contenido del documento firmado electrónicamente son idénticas o, no siéndolo, una se puede deducir de la otra (**anexo XVIII**)[454]. Para ello, es preciso que ambas partes (cuya relación en este tipo de casos suele basarse, por razones evidentes, en la confianza) se pongan de acuerdo con carácter previo sobre la clave en cuestión, que se almacenará por partida doble. Como bien puede

Creaciones Copyright, 2004, pp. 347 a 405. Por último, para una concepción integral de la seguridad electrónica y del encaje de la criptografía dentro de ella, *vid.* ILLESCAS ORTIZ, R., «La firma electrónica y el Real Decreto-ley 14/1999 de 17 de septiembre», cit., pp. 1 a 14; MOLINA MATEOS, J. M., «Libertad informática y criptología», *Informática y Derecho: revista iberoamericana de Derecho informático*, vol. 12, 1996, pp. 971 a 982.

[453] DI COCCO, C. Y OTROS, *Temi di Diritto dell'informatica*, cit., pp. 31 a 36.

[454] CIACCI, G., *La firma digitale*, cit., pp. 71 a 75; DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 521; GONZÁLEZ DE ALAIZA CARDONA, J. J./PERTÍÑEZ VÍLCHEZ, F., «Los contratos de adhesión y la contratación electrónica», en BERCOVITZ RODRÍGUEZ-CANO, R./MORALEJO IMBERNÓN, N. I./QUICIOS MOLINA, M. S. (coords.) *Tratado de los contratos*, Valencia, Tirant lo Blanch, 2013, p. 1792; GONZÁLEZ NAVARRO, F., «Comentario al art. 45 de la Ley de régimen jurídico de las Administraciones públicas y procedimiento administrativo común», cit., p. 39; MADRID PARRA, A., «Aspectos jurídicos de la identificación en el comercio electrónico», en ILLESCAS ORTIZ, R./RAMOS HERRANZ, I. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, p. 193; PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», cit., p. 496; VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., pp. 144 y 145.

comprenderse, cuanto mayor sea la longitud de la clave (medida en *bits*[455]), mayor será la seguridad del sistema[456].

El principal impedimento de este método de seguridad de la información es el riesgo derivado de que la contraparte, conocedora de la misma clave, facilite (voluntaria o forzadamente) la clave a terceros ajenos a la operación[457]. A ello se añade la posibilidad de rechazo, pues tanto el emisor como el receptor, conocedores de la clave única, podrían modificar el contenido del documento y firmar el documento con dicha clave, atribuyendo después a la otra parte la autoría de la firma electrónica; en este caso, el tercero ajeno a la relación no estaría en condiciones de poder determinar qué parte lo hizo, de modo que emisor y destinatario podrían rechazar el mensaje de datos negando su autoría[458]. Por tanto, es preferible que cada interviniente en la relación conozca su respectiva clave para que la integridad, confidencialidad y no rechazo del mensaje de datos puedan quedar, en gran medida, salvaguardados[459].

---

[455] Aludiendo, de nuevo, a la RAE, el *bit* es una «[u]nidad de medida de cantidad de información, equivalente a la elección entre dos posibilidades igualmente probables».

[456] ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 46.

[457] *Ibid.*, pp. 45 y 46. En torno a las principales vulnerabilidades de este sistema, *vid.* ADIEGO RODRÍGUEZ, J., «Problemática informática de la protección de obras digitales protegidas», cit., pp. 27 a 29.

[458] No obstante, cabría eliminar el problema del no rechazo. MARTÍNEZ NADAL, A., *Comercio electrónico, y autoridades de certificación*, Madrid, Civitas, 2000, p. 47, señala el supuesto en que «[…] dos partes (A y B) que desean comunicarse utilizando criptografía simétrica, comparten una clave común no entre ellas sino con una tercera parte de confianza, a la que envían el mensaje cifrado con la respectiva clave compartida con ella. Así, A, una de las partes, no podrá rechazar un mensaje alegando que ha sido cifrado por B, sino que en tal caso la tercera parte de confianza con la que comparte la clave secreta intervendrá para demostrar que tal mensaje fue cifrado efectivamente por A (y que no pudo ser cifrado por B, que, con este sistema, no comparte la clave con A sino con la tercera parte)».

[459] PEDRERO ESTEBAN, A., «Internet: cuestiones de seguridad en la Red», en FLECHA ANDRÉS, J. R. (coord.) *Marketing y recursos humanos*, Salamanca, Universidad Pontificia de Salamanca e Instituto de Estudios Europeos y Derechos Humanos, 2001, p. 60.

### 1.2. Criptografía asimétrica: especial atención a la firma digital

Un avance considerable en el ámbito de la criptografía tiene lugar con el desarrollo de la conocida como *criptografía asimétrica* o *de clave pública*, que permite el intercambio de información cifrada sin necesidad de que los intervinientes compartan una clave secreta común fijada previamente[460]. En concreto, el cifrado de clave asimétrica pública del receptor se fundamenta en la utilización de pares de claves para el envío de documentos firmados electrónicamente: una clave privada (también conocida como *clave de creación matemática*), tan sólo conocida por su titular y que ha de mantenerse en secreto en todo momento a fin de evitar el riesgo de que sea utilizada por quien no es su legítimo titular, con los consiguientes problemas de responsabilidad que ello podría implicar[461]; y una clave pública (también conocida como *clave de verificación matemática*), susceptible de ser conocida por cualquier persona, ya sea una o varias[462]. Pese a que ambas claves se hallan matemáticamente relacionadas, el diseño y la ejecución en forma segura de un criptograma asimétrico hace virtualmente imposible que las

[460] En opinión de autores como ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 37, la firma electrónica basada en criptografía asimétrica presenta elevadísimas dosis de seguridad, muy superiores a la firma manuscrita; en la misma línea, COMANDÉ, G. Y OTROS, *Il commercio elettronico: profili giuridici*, cit., p. 103.

[461] RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., p. 46. Como apunta BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 412, «[…] puede ocurrir, incluso, que ni siquiera el titular la conozca, pues probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal o a través del reconocimiento de la huella dactilar».

[462] ALCOVER GARAU, G., «La firma electrónica como medio de prueba», *Cuadernos de Derecho y comercio*, vol. 13, 1994, pp. 11 a 42; ALMONACID LAMELAS, V. Y OTROS, «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», cit., p. 431; BRAZELL, L., «Electronic security: encryption in the real world», *European intellectual property review*, vol. 21, 1999, pp. 17 a 27; MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., pp. 130 y 131; MARTÍNEZ NADAL, A., «La ley española de firma electrónica (Real Decreto Ley 14/1999)», en ILLESCAS ORTIZ, R./RAMOS HERRANZ, I. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, pp. 77 y 78; MARTÍNEZ NADAL, A., «Firma electrónica», en BOTANA GARCÍA, G. A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, p. 160; SALVADOR AYESTARÁN, I., «La firma digital: una tecnología para la intercomunicación en la sociedad-red», *Revista española de documentación científica*, vol. 1, 2001, p 3; SORIANO MALDONADO, S., «La firma electrónica en la UE y España: panorama del marco regulatorio general», *Economía industrial*, vol. 338, 2001, p. 80.

personas que conocen la clave pública puedan derivar de ella la clave privada (inderivabilidad)[463]. En estos casos, la comunicación responde a la siguiente dinámica: el emisor utiliza la clave pública del receptor (puesta a disposición por este, con carácter previo, bien de manera directa, bien facilitándola en su propio sitio web) para cifrar un documento electrónico que únicamente el receptor podrá descifrar con su correspondiente clave privada (**anexo XIX**)[464]. Este proceso se asemeja con el buzón físico dotado de una ranura de correo: la abertura está expuesta y accesible al público en general (siendo el lugar en que se encuentra el equivalente, en términos electrónicos, a la clave pública), de modo que alguien que conozca la dirección en que se ubica podrá acudir y colocar un mensaje escrito en su interior, siendo sólo la persona que posee la llave (en el supuesto presente, la clave privada) la única que podrá abrirlo y leer la información en él contenida. Con ello, se consigue que el mensaje de datos no sufra cambios (y, por tanto, no se conozca) a lo largo del proceso de envío y recepción (integridad) y que tan sólo el receptor legítimo (único en posesión de la clave privada correspondiente a esa concreta clave pública, que se autentica al ejecutar el proceso de coincidencia de claves, garantizando, así, la identificación autenticada del receptor y el no repudio en destino) puede leer el contenido de dicho mensaje, no pudiendo ser descifrado, ni siquiera, por la persona que lo envió (confidencialidad)[465].

---

[463] GARCÍA VIADA, C./GOMÁ LANZÓN, F., «Libro blanco de la firma electrónica notarial», *Revista jurídica del notariado*, vol. 45, 2003, p. 271; MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 79; MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», cit., p. 221.

[464] ADIEGO RODRÍGUEZ, J., «Problemática informática de la protección de obras digitales protegidas», cit., p. 30.

[465] La integridad conlleva la certeza de que el mensaje de datos recibido por el destinatario es, exactamente, el mensaje de datos enviado por el emisor, sin que haya sufrido alteración alguna durante el proceso de transmisión; de acuerdo con el artículo 3.6) del anexo DCMRI (DOUE L 251, de 27 de julio de 2004, p. 11), la integridad es «[…] el hecho de que la información contenida en el documento y los metadatos que la acompañan es completa (todos los datos están presentes) y exacta (los datos no presentan cambios)». Por su parte, la identificación autenticada del receptor implica poder atribuir de forma indubitada el mensaje electrónico a una determinada persona como receptora del mismo. El no repudio en destino supone que el receptor del mensaje de datos no puede negar, en ningún caso, que dicho mensaje haya sido enviado por él. Por último, la confidencialidad determina que el mensaje electrónico no ha podido ser leído por terceras personas distintas del emisor y del receptor durante el proceso de transmisión; sobre esta cuestión, *vid.* FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 38.

Sin embargo, con este método no existe manera de saber si el emisor del mensaje de datos es quien dice ser (identificación autenticada del emisor). La firma digital[466] viene a solucionar

[466] No existe en nuestro ordenamiento jurídico interno (tampoco en Derecho comunitario) una definición de firma digital. Sin embargo, países como Italia sí que han procedido a conceptualizar esta importante noción; de acuerdo con el artículo 1.s) CAD –con anterioridad, artículo 1.1.n) DPRDA– procedió a incorporar una definición de firma digital como «n) […] un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici», es decir, «[…] un particular tipo de firma electrónica cualificada basada en un sistema de claves criptográficas, una pública y una privada, correlativas entre sí, que permiten al titular mediante clave privada y al destinatario mediante la clave pública, respectivamente, hacer manifiesta y verificar la proveniencia y la integridad de un documento informático o de un conjunto de documentos informáticos». Además, complementando el artículo 1 CAD (con anterioridad, artículo 22 DPRDA), se entenderá por «h) chiave privata: l'elemento della coppia di chiavi asimmetriche, utilizzato dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico; i) chiave pubblica: l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal titolare delle chiavi asimmetriche», traducido al español, se entenderá «h) clave privada: el elemento de la pareja de claves asimétricas, utilizado por el sujeto titular, mediante el que se coloca la firma digital sobre el documento informático; i) clave pública: el elemento de la pareja de claves asimétricas destinado a ser conocido por el público, con el que se verifica la firma digital colocada sobre el documento informático del titular de las claves asimétricas». Ambos apartados h) e i) quedarán derogados con posterioridad. Para un estudio más profundo de esta figura dentro del Derecho italiano, *vid.* FINOCCHIARO, G. D., «La firma digitale: formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici», cit., pp. 112 a 149; FINOCCHIARO, G. D. Y OTROS, *Diritto dell'informatica*, cit., pp. 309 a 319; ROSELLO, C. Y OTROS, *Commercio elettronico, documento informatico e firma digitale: la nuova disciplina*, cit., pp. 536 a 540. Como podemos observar, la firma digital viene a ser una vehiculación de la firma electrónica a través de un método de cifrado específico: la criptografía asimétrica pública del emisor. En palabras de ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 37, «[…] la firma electrónica es el género y la digital, la especie; de modo que la firma electrónica incluye la firma digital, la cual está realizada mediante algoritmos de clave asimétrica»; en la misma línea, ALAMILLO DOMINGO, I., «Tipología legal de la firma electrónica en la Unión Europea», *Revista de la contratación electrónica*, vol. 23, 2002, p. 2; DE MIGUEL ASENSIO, P. A., «Regulación de la firma electrónica: balance y perspectivas», cit., p. 4; GOMES SOARES, F. S., «La prueba en la contratación electrónica de consumo», cit., p. 16; MARTÍNEZ NADAL, A., *Comercio electrónico, firma digital y autoridades de certificación*, cit., p. 42; PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», cit., p. 495; PLAZA PENADÉS, J., «La firma electrónica (regulación en España y en la Unión Europea)», cit., p. 417; RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., p. 47. En consecuencia, no podemos incurrir en el error, a veces detectado, de emplear los términos firma electrónica y firma digital como sinónimos o equivalentes. En contra de esta identificación, entre otros, MARTÍNEZ NADAL, A., «Comentarios de urgencia al urgentemente aprobado Real Decreto-ley 14/1999 de 17 de septiembre, sobre

este problema, y lo hace partiendo del método de criptografía de clave pública antes descrito, pero del modo inverso[467]. Ahora, el emisor cifra el documento electrónico con su propia clave privada (que genera una serie ininteligible de números y letras que representan la firma, diferente para cada documento que se firma[468]), pudiendo ser descifrado tan sólo por quien se encuentre en posesión de la correspondiente clave pública, también propiedad del emisor[469], que está matemáticamente relacionada con la primera y a la que puede acceder cualquier persona. De este modo, si con la clave pública del emisor se consigue desencriptar el contenido del documento electrónico, eso significa que el mismo se cifró con la clave privada de dicho emisor, que tan sólo él posee. En otras palabras, aplicando el emisor la clave privada sobre el conjunto de datos a transmitir, estos son encriptados o codificados, haciéndolos incomprensibles; después, en destino, el receptor aplica la clave pública que le ha proporcionado el emisor, consiguiendo la desencriptación de los datos transmitidos y retrocediendo, pues, hasta el mensaje inicial en claro[470]. Este método equivaldría al sellado de un sobre físico con un sello personal: el contenido del sobre (en nuestro caso, formato electrónico en el que se encuentra el mensaje de datos) puede ser abierto por cualquiera, pero la existencia del sello autentica al remitente. Gracias a este procedimiento, nos aseguramos de que el documento no se ha visto modificado respecto de su versión original, ya que, de haberlo sido, el resultado de la validación no sería correcto (integridad), pues cualquier variación en su contenido

---

firma electrónica», cit., p. 1861; MORENO NAVARRETE, M. Á., *Contratos electrónicos*, cit., p. 105; a favor de la misma, principalmente, FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 34.

[467] Por ello, y para diferenciarlo del anterior (al que atribuimos el nombre de *cifrado de clave asimétrica pública del receptor*), denominaremos este método como *cifrado de clave asimétrica pública del emisor*, denominación hasta ahora nunca empleada por la doctrina.

[468] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 118.

[469] FIORELLI, G. I., *Il contratto elettronico tra armonizzazione materiale e Diritto internazionale privato*, cit., pp. 97 a 99; VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., pp. 132 y 133.

[470] MORENO DELGADO, M. Y OTROS, «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», cit., p. 199. En términos similares, RUBIO TORRANO, E., «Firma electrónica», *Aranzadi civil*, vol. 13, 1999, p. 11, quien señala que por firma digital «[…] suelen entenderse ciertos procedimientos mediante los cuales alguien encripta […] un mensaje informático utilizando una clave privada que sólo él conoce, lo envía a su receptor a través de la red y da a conocer a éste una clave pública mediante la cual dicho receptor desencripta el mensaje y puede comprobar la identidad del emisor y la autenticidad del mensaje».

desembocaría en una alteración del algoritmo empleado para poder cifrarlo[471]. También comprobamos que el mensaje sólo puede ser enviado por el emisor[472], que se autentica en el momento en el que el receptor utiliza la clave pública adecuada (identificación autenticada del emisor y no repudio en origen)[473], consiguiendo efectos tanto o más útiles, en términos

[471] VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., p. 163.

[472] En otras palabras, tal como expone DÍAZ MORENO, A., «Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica», *Revista de la contratación electrónica*, vol. 2, 2000, p. 27, «[…] si la firma de un mensaje está creada con la clave secreta de [A] (en suma, es la firma digital de [A], ya que la probabilidad de que otro sujeto tenga la misma clave secreta resulta despreciable), parece claro que debe asumirse, al menos presuntamente que [A] es el autor de dicho mensaje y que éste refleja lo que fue su voluntad en el momento de firmar». Pese a ello, como bien indican BARREIROS FERNÁNDEZ, J., «El papel del notariado en el uso de la firma digital», *Notariado y contratación electrónica*, vol. 1, 2000, p. 19 y FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 48, la firma electrónica, a diferencia de la firma manuscrita, no es inescindible de la persona, ya que puede separarse el soporte físico de generación de su titular y ser suplantado por otra persona distinta sin que ello infiera apariencia alguna de anormalidad; bien es cierto, añaden, que la firma manuscrita también puede ser falsificada, pero existe una mayor dificultad si se emplean los mecanismos periciales oportunos. En la misma línea, BAUZÁ MARTORELL, F. J., «Las notificaciones telemáticas como fórmula de modernización de la oficina judicial», en AA.VV. (coord.) *Estudios acerca de la reforma de la justicia en España*, Madrid, Real Academia de Jurisprudencia y Legislación y Ministerio de Justicia, 2004, pp. 464 y 466, quien afirma que la firma electrónica es un mecanismo separado de la persona y, por consiguiente, puede ser utilizado por otra distinta del titular, de modo que «[…] habrá que admitir que, si la firma manuscrita implica forzosamente que el firmante vive al tiempo de estamparla, nada impide que una persona fallecida pueda firmar electrónicamente un documento» (obviamente, no ella, pero sí otra que utilice sus medios técnicos, pudiendo llegar a ser admitida como si así hubiera sido); esto, en opinión de RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., p. 44, permite defender lo acertado de la definición proporcionada por el artículo 3 LFE al referirse al *firmante* del documento y no al *autor/es* del mismo –como hacía el artículo 2.a) RDLFE–, pues, como acabamos de ver, la firma electrónica puede ser utilizada por terceras personas. En la misma línea, hay también quien diferencia el *firmante* del *suscriptor*, entendiendo por firmante la concreta persona física que estampa la firma y por suscriptor la persona a la que se atribuye la comunicación (ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 29).

[473] La identificación autenticada del emisor implica poder atribuir de forma indubitada el mensaje electrónico a una determinada persona como emisora del mismo, mientras que el no repudio en origen supone que el emisor del mensaje de datos no puede negar, en ningún caso, que dicho mensaje haya sido enviado por él (FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 38).

de validez y eficacia en el comercio y en los procedimientos legales, que la firma ológrafa en soporte físico y en formato papel[474].

En teoría, es posible cifrar el mensaje de datos completo y enviarlo al receptor para que este lo descifre. Sin embargo, en la práctica, dada la complejidad de la tecnología de cifrado asimétrico, este sistema conllevaría un empleo excesivo de tiempo y de capacidad informática[475]. Por ello, en todo procedimiento de estas características suele optarse por el cifrado, no del mensaje en claro como tal, sino de una parte resumida del mismo[476]; en concreto,

[474] MARTÍNEZ NADAL, A., «Firma electrónica», cit., p. 160; DE MIGUEL ASENSIO, P. A., «Regulación de la firma electrónica: balance y perspectivas», cit., pp. 6 y 7; GARCÍA MÁS, F. J./LÓPEZ-MONÍS GALLEGO, A., «La contratación electrónica: modernidad y seguridad jurídica», en F., D. DE M. J. (coord.) *Instituciones de Derecho privado*, Madrid, Civitas, 2004, p. 116; MERCHÁN MURILLO, A., *Firma electrónica: funciones y problemática. Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, cit., p. 68. Sin embargo, como podemos observar, el método de cifrado de clave asimétrica pública del emisor, a diferencia del método de cifrado de clave asimétrica pública del receptor, no resuelve dos problemas: de una parte, el no repudio en destino, que podría solventarse si las claves fueran propiedad del receptor; de otra, la confidencialidad, que quedaría garantizada, al igual que la anterior, si las claves estuvieran en poder del destinatario del mensaje de datos, ya que el documento electrónico, firmado por el emisor con la clave pública del receptor, sólo podría ser descodificado con la clave privada de este último, siendo, por tanto, sólo él el que podría llegar a conocer su contenido; sobre esta cuestión, *vid.* GARCÍA VIADA, C. Y OTROS, «Libro blanco de la firma electrónica notarial», cit., p. 301; MARTÍNEZ NADAL, A., *Comercio electrónico, firma digital y autoridades de certificación*, cit., pp. 45 a 63.

[475] CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 50.

[476] Para una descripción más completa del sistema que a continuación se describe, *vid.* ALCOVER GARAU, G., «La firma electrónica como medio de prueba», cit., pp. 19 y 20; CIACCI, G., *La firma digitale*, cit., pp. 81 a 84; COMANDÉ, G. Y OTROS, *Il commercio elettronico: profili giuridici*, cit., pp. 106 a 112; LOMASCOLO SZITTYAY, R., «Aspectos técnicos de la firma electrónica», en PÚBLICA, I. N. DE A. (coord.) *Firma digital y Administraciones públicas*, Madrid, Instituto Nacional de Administración Pública, 2003, pp. 29 a 81; MORENO DELGADO, M. Y OTROS, «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», cit., pp. 199 a 201; PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», cit., pp. 497 y 498; SORIANO MALDONADO, S., «La firma electrónica en la UE y España: panorama del marco regulatorio general», cit., p. 80; VILA SOBRINO, X. A., «Aspectos técnicos para el desarrollo de aplicaciones de comercio electrónico», en TATO PLAZA, A./ALBOR BALTAR, Á. F. (coords.) *Comercio electrónico en Internet*, Madrid, Marcial Pons, 2001, pp. 62 a 66.

antes del momento de envío, se aplica una función algorítmica, conocida como *hash*[477], que extrae de cada mensaje de datos específico una longitud fija (habitualmente menor que la del documento original) y representativa del mismo, sea cual sea la extensión del documento que se va a enviar[478]. Este resumen o extracto, que se conoce como *huella digital*, está conformado por un listado de letras y números por completo incomprensible, resultado de aplicar el algoritmo al mensaje de datos que se quiere transmitir. Esta huella digital se caracteriza por su irreversibilidad (a partir de ella no es posible acceder al mensaje de datos en claro y descifrarlo) y por su exclusividad (sólo existe una para cada mensaje de datos)[479], de forma que, modificando tan sólo una de las letras o números que la integran, el resultado sería completamente diferente al existente con carácter previo.

Una vez obtenida la huella digital, se encripta, aplicando la clave privada del firmante (en nuestro caso, como veremos, datos de creación de firma electrónica) por medio de un sistema informático (dispositivo de creación de firma electrónica) y obteniendo un mensaje de datos cifrado que se considera la firma electrónica del documento en claro, que será diferente para cada mensaje de datos, ya que depende de este[480]. Sendos mensajes de datos, el inicial u original, total y en claro, y la huella digital cifrada, son remitidos conjuntamente por el emisor y

---

[477] La Recomendación UIT-T.X.810, p. 3, define el *hash* como la característica de un ítem de datos, por ejemplo, un valor de comprobación criptográfico o el resultado de la ejecución de una función de cálculo unidireccional sobre los datos, que es suficientemente peculiar del ítem de datos y que no es factible, mediante cálculo, hallar otro ítem de datos que posea la misma característica. De igual modo, define la función unidireccional como aquella función (matemática) cuyo cálculo es fácil pero que, cuando se conoce un resultado, no es factible, mediante cálculo, hallar cualquiera de los valores que pueden haber sido suministrados para obtenerlo.

[478] GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, cit., p. 58.

[479] DÍAZ MORENO, A., «Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica», cit., p. 21; FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 39.

[480] En otras palabras, como en su día indicara *Ibid.*, p. 39, existirán tantas firmas electrónicas como documentos electrónicos (distintos, claro) se envíen, luego la firma electrónica no es una firma como tal, pues no es una transposición digital de la firma manuscrita ni constituye, a diferencia de esta, algo (con matices) invariable; lo mismo afirma BONARDELL LENZANO, R., «La firma electrónica: especial consideración de sus efectos jurídicos», *Notariado y contratación electrónica*, vol. 1, 2000, p. 61, según el cual «[…] el mecanismo objeto de análisis no es propiamente una firma en el sentido que lo es la autógrafa, sino un procedimiento generador de una

firmante al receptor, además de la clave pública (datos de verificación o validación de firma electrónica) de la que es propietario.

A continuación, el destinatario procede con la verificación de la firma electrónica, que no es sino un proceso de comprobación de la misma por referencia al documento electrónico original y a la clave pública dada, concluyendo de esta forma si la firma electrónica fue creada para ese concreto mensaje de datos en función de la correspondencia de claves. Para obtener este resultado, el receptor llevará a cabo dos operaciones: en primer lugar, descodificará la huella digital cifrada y firmada con la clave privada del firmante, aplicando a tal fin la clave pública, también propiedad de este, y obteniendo, de nuevo, la huella digital inicial –a la que denominaremos, para una mejor comprensión, *huella digital final (1)*–; en segundo lugar, empleará nuevamente la función *hash* al documento electrónico original para obtener una nueva huella digital del mismo –*huella digital final (2)*–: si ambas huellas digitales –*huella digital final (1) y huella digital final (2)*– coinciden, podemos concluir que el documento electrónico inicial que se envió es el mismo que se ha recibido (integridad y no repudio en origen) y que este ha sido firmado por el emisor con ese mismo contenido, emisor que, por ende, queda autenticado como titular de las claves, pública y privada, utilizadas para la firma electrónica (identificación autenticada); en cambio, si no coinciden, se entiende que ha habido cambios y, por ende, alguna manipulación en el íter de la comunicación, no pudiendo confiar en el contenido del documento, bien porque este ha sido alterado, bien porque el titular de la clave privada con la que se firmó no es el mismo que el titular de la clave pública con la que se trató de descifrar (**anexo XX**)[481]. Dadas estas circunstancias, el firmante que niegue haber firmado el documento al cual se halla adjuntado una firma electrónica creada a partir del mismo con una clave privada que se corresponde con la clave pública que verifica dicha firma tendrá que probar tal circunstancia[482]. Esta presunción se asienta sobre el hecho de que, llegado el caso, el firmante aparente tiene una mayor facilidad a la hora de aportar los medios de prueba que

apariencia jurídica (la propia firma electrónica) a la que se asocian unos efectos parcialmente semejantes a los de aquella».

[481] PEDRERO ESTEBAN, A., «Internet: cuestiones de seguridad en la Red», cit., p. 63.

[482] ALCOVER GARAU, G., «Concepto de firma electrónica, firma electrónica y firma manual», en PERALES SANZ, J. L. (coord.) *La seguridad jurídica en las transacciones electrónicas: Seminario organizado por el Consejo General del Notariado en el UIMP*, Madrid, Civitas, 2002, p. 35; ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., pp. 58 y 59.

resulten necesarios para negar su intervención (por ejemplo, sustracción de la clave privada), en tanto que para el receptor del mensaje de datos (partiendo de que actúa con buena fe) será mucho más difícil poder probar que el firmante aparente fue realmente el que firmó el documento[483]; además, dado que, en principio, es el firmante titular del par de claves el encargado de la custodia de las mismas, parece justo que sobre él deba recaer la responsabilidad de su adecuada protección[484].

En definitiva, para la validez y eficacia de la firma electrónica que emplee este método de cifrado criptográfico asimétrico, resultará imprescindible que, en el proceso de generación del par de claves, se cumplan una serie de características que hagan que las mismas estén dotadas de niveles mínimos de calidad y de seguridad, evitando que sean rompibles o reproducibles (en el sentido de que, a partir de una de ellas –en este caso, de la clave pública–, pueda obtenerse la otra –clave privada–, en lo que se conoce como *viabilidad computacional*, que dependerá de factores como la longitud de la clave, los avances de la técnica, la capacidad del sistema encargado de protegerlas o el coste y el tiempo necesarios para atacar los datos que las conforman[485]), previsibles (es decir, fácilmente conocibles por el proveedor del *software* o del *hardware* que haga posible la generación de las claves, reconstruyendo el proceso de creación), repetibles (por no introducir los correctores de aleatoriedad adecuados en los procedimientos de formación) o carentes de unicidad (por existir una misma clave para dos o más personas)[486].

---

[483] DÍAZ MORENO, A., «Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica», cit., pp. 27 y 28.

[484] *Ibid.*, p. 17.

[485] 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, cual es que, una vez que se multiplican entre sí para producir un nuevo número, es virtualmente imposible determinar cuáles fueron los dos números primos que crearon ese nuevo número de mayor longitud. En consecuencia, aunque muchas personas conozcan o puedan conocer la clave pública del firmante y la utilicen para verificar sus firmas electrónicas, no podrán descubrir la correspondiente clave privada de aquel y utilizarla con fines falsificadores.

[486] MARTÍNEZ NADAL, A., «La ley española de firma electrónica (Real Decreto Ley 14/1999)», cit., pp. 80 a 82; MARTÍNEZ NADAL, A., «Firma electrónica», cit., pp. 169 y 170; MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., pp. 461 y 462. En esta última obra, esta autora añade que estos requisitos de calidad y de seguridad a cumplir por las claves criptográficas pueden variar en función del sistema de creación

No obstante, aun expuestos de manera separada ambos métodos criptográficos asimétricos anteriores, en el fondo ambos podrían realizarse de manera conjunta a través de dos cifrados secuenciales. En efecto, en un primer paso, el emisor cifraría el mensaje de datos con su clave privada, dando lugar a la firma electrónica, que garantizaría la identificación autenticada del firmante y la integridad y el no repudio en origen del contenido del documento una vez descifrado este con la clave pública de la contraparte; después, en un segundo paso, el firmante cifraría el mensaje de datos con la clave pública del destinatario, mensaje de

---

de las claves; en concreto, indicando la dualidad que suele existir al respecto, señala que «[…] existen dos alternativas básicas en función de dónde se genera el par de claves, por el propio titular o por una entidad distinta. A favor del sistema central de creación de claves por una entidad distinta del titular (p. ej., una entidad de certificación) se alega que ofrece la ventaja de que los instrumentos de generación utilizados por la entidad serán normalmente de mayor calidad y ofrecerán mayores garantías que los que pueda utilizar un simple particular. No obstante, el inconveniente de este sistema central frente al sistema local de creación por el propio titular es que no existe garantía de la destrucción efectiva, por parte de la entidad de certificación, de la clave privada de firma, dando pie a posibles utilizaciones fraudulentas» (*Ibid.*, p. 464). Pese a ello, parece ser que, junto con la generación, también existe la posibilidad de que el PSSIic gestione los datos de creación de firma electrónica, ya sean estos generados previamente, o no, por el mismo PSSIic; así parece deducirse, en el Derecho comunitario, de la DFE, que permite inicialmente la generación y la gestión únicamente a los PSSIic que expidan certificados reconocidos –letras g) y j) del anexo II–, es decir, a PSSIic reconocidos. En cambio, la situación originaria en nuestro país parece ser algo distinta, ya que el artículo 12.f) RDLFE admitía el precitado sistema central sólo en favor de PSSIic reconocidos, si bien parecía permitir la gestión de los datos de creación de firma electrónica también a aquellos PSSIic que no lo fueran, estableciendo, en este caso, la obligación de «[…] no almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo que ésta lo solicite», de modo que, si entre estos servicios se encontraban los de gestión, sólo se permitía almacenar estos datos a solicitud del usuario. Más tarde, con la LFE, volvemos a la situación marcada por la DFE, pues sólo se permitirá a los PSSIic reconocidos tanto la generación –artículo 20.e)– como la gestión –artículo 18.a)– de los datos de creación de firma electrónica, sustituyendo, además, el inciso final del artículo 11.2.c) RDLFE en el que se permitía el almacenamiento o la copia de dichos datos de creación si la persona a la que el PSSIic había prestado sus servicios así lo solicitaba por un nuevo inciso final en el que ello se permite siempre que el servicio prestado consista en la gestión, con independencia de que exista solicitud alguna por parte del usuario. En la actualidad, el apartado 3 del anexo II RIE-SCTE sólo permite la generación y la gestión de los datos de creación de firma a PSSIisc que sean cualificados; no obstante, el artículo 11.2.a) ALSEC, entrando, en principio, abiertamente en contradicción con el contenido del Reglamento europeo, permite la gestión a todo PSSIisc, permitiéndole el almacenamiento y la copia de los datos de creación de firma electrónica cuando lleve a cabo esta actividad.

datos que, una vez descifrado por el receptor con su correspondiente clave privada, posibilitaría el no repudio en destino y la confidencialidad del documento[487].

2. Certificados de firma electrónica

Pese a que el sistema de firma digital *supra* descrito garantiza que el mensaje de datos verificado adecuadamente por el receptor mediante el empleo de la clave pública del emisor se ha firmado con la correlativa clave privada de este, no permite comprobar un extremo fundamental, como es el de la confirmación de la verdadera identidad del firmante. Y ello porque, aun cuando las claves (pública y privada, o, lo que es lo mismo, los datos de creación y de verificación o validación de firma electrónica, respectivamente), se correspondan matemáticamente, no hay asociación intrínseca con una persona física específica, no existiendo, por ende y consecuentemente, seguridad de que las claves sean titularidad del sujeto que las posee, ya que el verdadero propietario puede haber sido suplantado por un tercero que, en su nombre, lleve a cabo el empleo del par de claves para la firma electrónica de documentos[488].

Así, mientras que este sistema de identificación y autenticación no presenta mayores problemas en aquellos supuestos en que la clave pública es conocida ampliamente en el mercado o cuando el titular de la firma electrónica ha comunicado con carácter previo al destinatario la clave pública que se corresponde con la clave privada, de modo que este último tiene certeza de que quien firma electrónicamente es realmente quien dice ser (sería así cuando la entrega de la clave pública se ha realizado personalmente y las partes de la comunicación se conocen previamente), sí lo hará en aquellos casos en que su utilización tenga lugar en un entorno de comercio electrónico generalizado y en redes abiertas como Internet[489]; en este

[487] Sobre esta posibilidad, *vid.* MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., p. 241; ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 44; PEÑA LÓPEZ, I., «Fundamentos tecnológicos del Derecho de la sociedad de la información», cit., p. 101; RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., pp. 46 y 47; SANJURJO REBOLLO, B., *Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, protección de datos, negocios audiovisuales, e-commerce, consumidores, marketing*, cit., pp. 516 y 517.

[488] MARTÍNEZ NADAL, A., «Firma electrónica», cit., p. 161.

[489] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 133; JULIÀ BARCELÓ, R., *Comercio electrónico entre empresarios: la formación y prueba del contrato electrónico (EDI)*, cit., p. 240.

último contexto, es muy probable que las partes no se conozcan con anterioridad ni que concurran en un mismo tiempo y lugar para poder identificarse e intercambiar las claves que utilizarán a partir de ese momento.

Para poner remedio a la situación de incertidumbre que, inevitablemente, genera el empleo de la firma electrónica entre partes desconocidas y geográficamente distantes, la criptografía asimétrica se hace acompañar de unos instrumentos complementarios que a aquella imprimen mayores dosis de fiabilidad: son los conocidos como *certificados de firma electrónica*[490]. Son, estos, documentos electrónicos de naturaleza privada emitidos por PSSIisc (antes, PSSIic, siempre, *autoridades de certificación*[491]), quienes en el contexto de lo que conocemos como *infraestructura de clave pública* (PKI)[492], certifican y respaldan con su propia clave privada

[490] Pese a ello, y en otro orden de cosas, resulta adecuado poner de manifiesto una circunstancia importante, ya apuntada por ALMONACID LAMELAS, V. Y OTROS, «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», cit., pp. 434 y 435, en los siguientes términos: «[l]a aparición y regulación de los certificados electrónicos […] ha supuesto una indudable afectación a alguna de las funciones de la fe pública, como es la verificación de la identidad del otorgante. En este sentido, ya se ha producido la sustitución de la legitimación notarial de la firma manuscrita de un documento por la verificación del certificado electrónico que refrenda la firma electrónica reconocida o cualificada, como en el caso del depósito de cuentas anuales de las compañías mercantiles en el Registro Mercantil». Por lo demás, recoge CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 57, tradicionalmente, se han ofrecido tres soluciones para salvaguardar la correspondencia entre identidad real y entidad comunicada en el mensaje de datos a través de la firma electrónica, siendo la última de ellas la más aceptada o frecuente: «[…] a) la existencia de un registro de claves públicas que case las claves públicas con las identidades reales, protegiendo al tercero, bien por la fe pública registral (si se trata de un registro público), o bien mediante una función asegurativa (si se trata de una entidad privada); b) el recurso a una *Web-of-trust*, como la utilizada en el conocido programa de encriptación PGP (*Pretty Good Privacy*) a la que el receptor de un mensaje puede dirigirse para comprobar (no existe una función asegurativa) si la entidad del firmante es correcta, según las declaraciones de terceros que ya han contratado confiados en esta firma; c) la utilización de terceras partes de confianza, autoridades de certificación o prestadores de servicios de certificación, empresas que comprueban por sí mismas o a través de una "autoridad de registro local" la verdadera identidad del firmante y origina para éste una firma digital»; en la misma línea, MARTÍNEZ NADAL, A., *Comercio electrónico, firma digital y autoridades de certificación*, cit., pp. 66 a 68.

[491] También recibe otras denominaciones, como la de *proveedor de servicios de certificación*, en Derecho comunitario, o la de *entidad de certificación*, en los trabajos iniciales de UNCITRAL, si bien en el texto definitivo de la LMFE se impuso y consolidó la denominación, arriba apuntada, de PSSIic.

[492] ADIEGO RODRÍGUEZ, J., «Problemática informática de la protección de obras digitales protegidas», cit., pp. 30 a 33; GARCÍA VIADA, C. Y OTROS, «Libro blanco de la firma electrónica notarial», cit., p. 284; RICO CARRILLO,

la identidad digital de personas y la autenticidad de las comunicaciones y documentos que estas puedan llegar a generar[493].

Así, previa comprobación de la identidad del solicitante de la certificación (firmante), se hace constar que este es, efectivamente, el propietario de una determinada clave pública[494] y no un tercero suplantador (**anexo XXI**), generando la confianza necesaria en los terceros usuarios (también conocidos como *parte usuaria* o *terceros que confían* en el certificado electrónico) y asumiendo simultáneamente, al poner de manifiesto este extremo, una serie de obligaciones y una concreta responsabilidad por la emisión, en su caso, de certificados electrónicos incorrectos (titularidad de las claves por un tercero ajeno). Los certificados electrónicos podrán ser enviados al solicitante para que este los adjunte a los mensajes electrónicos que envíe o quedar como un registro en una base de datos del PSSIisc accesible a terceros[495],

M., «El Reglamento europeo sobre identificación y servicios de confianza electrónicos», cit., p. 20; VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., pp. 132 y 133.

[493] Pese a ello, advierte GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, cit., pp. 59 a 61, conviene ser cautelosos a la hora de afirmar que con esta PKI se garantiza plenamente la identidad de quien firma, ya que, aun cuando todo el proceso se haya desarrollado perfectamente y no se detecte alteración alguna, cabe la posibilidad de que el titular de la firma electrónica no haya sido la persona que haya firmado, sino un tercero, bien porque dicho titular le ha comunicado voluntariamente la clave privada, bien porque esta se ha extraviado, bien porque ha sido copiada maliciosamente; también existirá el caso de PSSIisc que suministren certificados electrónicos en un *software*, sin ninguna medida de seguridad o barrera de control adicional que impida el acceso a los mismos por quien no es su legítimo titular, almacenándose en el disco duro del ordenador de tal modo que cualquiera que entre en él puede hacer uso de dichos certificados (BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 430). En todos estos supuestos, y aplicado al supuesto de celebración de un contrato electrónico, resalta el primero de los autores que «[…] si una de las partes contratantes no ha sido quien ha firmado el documento, sino un tercero, no podemos decir que haya prestado su consentimiento en el contrato; podremos decir cualquier otra cosa, que asuma las obligaciones derivadas del mismo, que existe un principio general en la firma electrónica sobre asunción de lo que se firma, y un largo etcétera, pero nunca que efectivamente ha prestado el consentimiento».

[494] En cambio, no hace falta verificar la relación de esta clave pública con la clave privada, ya que se valida por construcción (PEÑA LÓPEZ, I., «Fundamentos tecnológicos del Derecho de la sociedad de la información», cit., p. 102).

[495] MARTÍNEZ NADAL, A., «Firma electrónica, certificados y entidades de certificación», cit., p. 206.

siendo aconsejable, de optar por esta última posibilidad, que el proceso de emisión del certificado electrónico garantice que el firmante conoce su contenido y le permita, en consecuencia, declarar (o aprobar tácitamente, con su empleo) que este es correcto[496].

Como podemos intuir, el método descrito garantiza la identidad de quien emite un mensaje de datos, merced a la plasmación de su clave pública, ya certificada por estar firmada con la clave privada del PSSIisc[497], pero no la identidad de la persona receptora del documento electrónico que autentica dicha clave pública, que no podrá hacer constar su verdadera identidad si no es con su correspondiente certificado electrónico. Así, resulta conveniente que, para establecer una comunicación segura entre los intervinientes (máxime si estos son contratantes), ambos cuenten con sus respectivos certificados electrónicos que acrediten que, estando *de facto* en posesión de las claves con las que llevan a cabo la correspondiente firma electrónica de documentos, son, *de iure*, los auténticos propietarios legítimos de las mismas y, por ende, los verdaderos autorizados para obligarse por el contenido de la información que emiten[498].

Los certificados de firma electrónica aparecen definidos en el artículo 3.14) RIE-SCTE como «[…] una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona»[499]. En

---

[496] CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 60.

[497] El certificado electrónico es firmado electrónicamente con la clave privada del PSSIisc, de modo que cualquiera que conozca su correspondiente clave pública puede (en mayor o menor medida, dependiendo de la seguridad que ofrezca esta firma electrónica) confiar en que dicho certificado electrónico es auténtico, de suerte que quien se halla en posesión del mismo y aparece en él identificado es quien dice ser (DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 526).

[498] *Ibid*., p. 525.

[499] En términos muy similares se pronunciaba el artículo 2.9) de la DFE, que por certificado electrónico entendía «[…] la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de esta»; en este caso, al igual que sucederá con el RDLFE y con la LFE, no se introduce la denominación *certificado de firma electrónica*, sino tan sólo la de *certificado*, por una razón obvia, y es que, en ese momento, sólo se regulaba la firma electrónica como único servicio de confianza. Por su parte, el artículo 2.b) LMFE definirá, en términos más generales, el certificado electrónico como «[…] todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma».

nuestro país, el RDLFE introdujo originariamente el concepto de certificación con una redacción prácticamente idéntica a la que después contuvo la DFE[500], siendo reemplazada posteriormente por aquella proporcionada por el artículo 6.1 LFE[501], más comprensible y adecuada y que define el certificado electrónico de forma tecnológicamente neutral[502] como el documento firmado electrónicamente[503] por un PSSIic que vincula unos datos de verificación de firma (clave pública) a un firmante y confirma su identidad. Se trata, pues, de documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su correspondiente identidad personal, dándole a conocer, de este modo, en el ámbito virtual como firmante.

### 2.1. Certificados electrónicos cualificados

Junto a la categoría general de certificado electrónico antes expuesta, la normativa diferencia otra a la que, por estar dotada de unos mayores requisitos de seguridad, atribuye una especial eficacia[504]. Estamos hablando de los conocidos como *certificados cualificados de firma electrónica*[505] (antes de la aparición del RIE-SCTE, *certificados reconocidos*), que, expedidos por PSSIisc cualificados, aportan un mayor plus de valor y seguridad, toda vez que se han emitido cumpliendo determinadas exigencias en lo que se refiere a su contenido, a los procedimientos

[500] «[…] la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad» –artículo 2.i) RDLFE–; esta redacción fue criticada por autores como ALAMILLO DOMINGO, I., «Tipología legal de la firma electrónica en la Unión Europea», cit., p. 10, pues contenía el objeto definido en la definición, «[…] lo que no dice gran cosa acerca del objeto en estudio».

[501] Y, con carácter previo, el apartado II de la Exposición de Motivos de la Ley, que, de forma general y remarcando su función identificativa, define los certificados electrónicos como aquellos «[…] documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante».

[502] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 135; MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», cit., p. 230.

[503] Son, por tanto, documentos electrónicos, como bien subraya DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 522.

[504] VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., p. 149.

[505] En mi opinión, hubiera sido más correcto (a costa, cierto, de incurrir en una cierta redundancia) hablar de *certificados cualificados de firma electrónica cualificada.*

de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica[506].

Más concretamente, los certificados cualificados de firma electrónica aparecen definidos en el artículo 3.15) RIE-SCTE –antes, en términos similares, en el artículo 2.10) DFE–, que, por tales, entiende aquellos certificados que cumplen dos requisitos básicos: de una parte, que hayan sido expedidos por un PSSIisc cualificado; de otra, que cumplan determinadas condiciones recogidas en su anexo I. Estas condiciones se circunscriben a: a) una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de firma electrónica –antigua letra a) del anexo I DFE–; b) un conjunto de datos que represente inequívocamente al PSSIisc cualificado que expide los certificados cualificados de firma electrónica, incluyendo, como mínimo, el Estado miembro en el que dicho PSSIisc cualificado está establecido y, caso de que sea una persona jurídica, el nombre y (cuando proceda) el número de registro según consten en los registros oficiales y, en el supuesto de que sea una persona física, el nombre –antigua letra b) del anexo I DFE–; c) al menos, el nombre del firmante o un seudónimo[507], indicándose este último hecho, en su caso, de forma clara –antigua letra c) del anexo I DFE–; d) datos de validación de la firma electrónica que correspondan a los datos de creación de la misma[508] –antigua letra e) del anexo I DFE–; e) datos relativos al inicio y al final del período de validez del certificado

[506] Apartado II de la Exposición de Motivos de la LFE. Consecuencia de esta distinción, autores como MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 137, critican la regulación, española y comunitaria, de los certificados electrónicos no cualificados, que, en ocasiones, no proporcionan una verificación fiable de la identidad (por lo que no cumplen su función) ni son, por ende, realmente certificados; en este sentido, añade, «[…] aunque desde el punto de vista comercial es comprensible que los prestadores ofrezcan distintos productos, con un distinto coste y también con un distinto nivel de seguridad, desde el punto de vista jurídico, esta diversificación comercial no puede llegar al punto de privar al certificado de su función básica y esencial de distribución segura de claves públicas y otros elementos de verificación de firmas electrónicas».

[507] Autores como Van Dellen, M., «Anonymity on the Internet. What does the concept of anonymity mean?», *Electronic Law Review*, vol. 9, 2002, pp. 1 a 6, sostienen que la posibilidad de realizar actos jurídicos a través de seudónimos, manteniendo el anonimato, es una de las características de los medios electrónicos de comunicación frente a los medios tradicionales. Sobre las maneras de mantener oculta la identidad en Internet, *vid.* BARRIUSO RUIZ, C., *La contratación electrónica*, cit., pp. 81 a 83.

[508] En el supuesto de claves asimétricas en que consiste la firma digital, este requisito queda satisfecho con la inclusión de la clave pública que se corresponde con la clave privada del titular de la firma electrónica y con el certificado electrónico.

electrónico[509] –antigua letra f) del anexo I DFE–; f) el código de identidad del certificado de firma electrónica, que debe ser único para el PSSIisc cualificado[510] –antigua letra g) del anexo I DFE–; g) la firma electrónica avanzada o, en su caso, el sello electrónico avanzado del PSSIisc cualificado expedidor[511] –antigua letra h) del anexo I DFE, si bien no recoge la figura

[509] Único supuesto, este, de extinción normal del certificado electrónico. En cualquier caso, como señala CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., pp. 76 y 77, pese a lo adecuado de esta previsión, «[…] es del todo incorrecto hablar de período de validez del certificado, pues esta expresión indica que, transcurrido el tiempo previsto o en cualquier otro de los supuestos […], el certificado pierde sus efectos, con lo que la firma, aun siendo avanzada, deja de estar certificada por un certificado y, por tanto, deja de ser una firma reconocida. En nuestra opinión tal concepto debería sustituirse por el de período operacional del certificado […]. De este modo, cualquier mensaje firmado durante el período operacional con una firma certificada con un certificado válido se considerará escrito firmado para siempre»; en la misma línea, RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., p. 71. En cualquier caso, esta condición legal nos lleva al problema de la determinación del momento en el que fue firmado un documento electrónico, pues, de otro modo, no podrá asegurarse *a priori* que la firma electrónica se creó estando vigente el certificado electrónico y que esta cumplía los requisitos para ser considerada segura, siendo adecuada a tal efecto la utilización de un sistema de sello temporal digital; sobre las utilidades y funcionamiento de los distintos sistemas de sello temporal, *vid.* FERRER GOMILA, J. L./MARTÍNEZ NADAL, A., «El problema temporal del sistema de certificados en el comercio electrónico», *Revista de la contratación electrónica*, vol. 1, 2000, pp. 29 a 47; VÁZQUE GARCÍA, R. J., «Tecnología digital y formalización contractual», *Informática y Derecho: revista iberoamericana de Derecho informático*, vol. 33, 2000, pp. 95 a 116. En este sentido, en el Reglamento eIDAS nace un servicio de confianza no regulado en la normativa anterior (cuestión esta criticada por autores como DÍAZ FRAILE, J. M., «Estudio de la regulación de la firma electrónica en la directiva europea de 13 de mayo de 1998», *La ley: revista jurídica española de doctrina, jurisprudencia y bibliografíaL*, vol. 6, 1998, p. 2151): el conocido como *sello de tiempo electrónico*, definido en el artículo 3.33) Reglamento eIDAS como los «[…] datos en formato electrónico que vinculan otros datos en formato electrónico con un instante concreto, aportando la prueba de que estos últimos datos existían en ese instante», siendo cualificado cuando cumpla los requisitos contenidos en el artículo 42 RIE-SCTE, que, junto con el artículo 41, se ocupan de su regulación.

[510] A diferencia del RIE-SCTE (y de la LFE), en la DFE no se establecía que el código identificativo del certificado electrónico debiera ser único. Sin embargo, entendemos que esta inclusión es muy positiva, dada la utilidad de dicho código, que debe servir para identificar el certificado electrónico en cuestión, no sólo del resto de certificados emitidos por un mismo PSSIisc, sino también de aquellos que sean expedidos por cualquier otro PSSIisc, de modo que no existan dos certificados electrónicos con códigos identificativos idénticos (MARTÍNEZ NADAL, A., *La Ley de firma electrónica*, cit., p. 107).

[511] Este requisito no exige que el PSSIisc cualificado que expide el certificado electrónico a favor del firmante firme con una firma electrónica cualificada; tan sólo es necesario que, para que pueda ser cualificado, firme el certificado electrónico con su firma electrónica avanzada. Sobre esto, tenemos que realizar las siguientes observaciones: de una parte, el certificado de firma electrónica es una declaración electrónica que vincula los datos

de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona; de otra, la firma electrónica avanzada es una firma electrónica que, entre otros aspectos, se caracteriza por estar vinculada al firmante de manera única. Pues bien, el hecho de que se imponga que el certificado electrónico cualificado haya de contar con la firma electrónica avanzada del PSSIisc cualificado, supone una vinculación de los datos de validación de esta firma electrónica avanzada con el PSSIisc persona física y una confirmación de, al menos, su nombre o su seudónimo. En ese caso, si se presupone la existencia de una entidad que ha de emitir a favor de este PSSIisc un certificado electrónico, no entiendo por qué dicho certificado no puede ser cualificado y, por ende, cualificada la firma electrónica que plasme dicho PSSIisc en el certificado electrónico que, a su vez, emita a favor del firmante último. Veámoslo con un ejemplo: A (firmante 1) solicita un certificado electrónico cualificado a B (PSSIisc 1 y firmante 2); para poder firmar electrónicamente el certificado electrónico cualificado solicitado por A, B ha de contar legalmente con una firma electrónica avanzada, lo que implica la existencia a su favor de un certificado electrónico expedido a su favor por C (PSSIisc 2 y firmante 3), que, entiendo, podrá expedir a favor de B un certificado electrónico que podrá ser cualificado (en cuyo caso, la firma electrónica de B, que habrá de plasmar en el certificado electrónico cualificado de A, podrá ser cualificada, siempre que también se haya creado mediante un dispositivo cualificado de creación de firma electrónica) o no cualificada (en cuyo caso, la firma electrónica de B que habrá de plasmar en el certificado electrónico cualificado de A sería avanzada). En ambos casos, para que B pueda firmar con una firma electrónica que, como mínimo, sea avanzada, ha de contar a su favor con un certificado electrónico expedido por otra entidad, desconociendo el motivo por el que no puede ser firma electrónica reconocida, o, pudiendo serlo, por qué no se exige en la letra g) del anexo I RIE-SCTE. Bien es cierto, como apuntara en su momento CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 88, que ello «[…] tiene la ventaja de que no se exige que el certificado de la firma electrónica del prestador de servicios de certificación sea reconocido […]. De este modo, el certificado de la firma utilizada por la entidad certificadora para firmar el certificado expedido por éste puede tener una duración superior». Por lo demás, sobre la cuestión de quién certifica a la entidad de certificación tuvo ocasión de pronunciarse MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., pp. 214 y 215, y lo hizo planteando las dos alternativas existentes en materia de política legislativa: «[e]n primer lugar, la certificación de la entidad de certificación por una entidad superior y distinta (que podría ser, aunque no necesariamente, una administración pública), con lo que se establecería una jerarquía de entidades de certificación; en segundo lugar, la denominada autocertificación que consistiría en prescindir de cualquier certificación formal y que sea el mercado el que valore la fiabilidad de una entidad de certificación en función de su prestigio y actuación. Y mientras el primer modelo de certificación necesita de una jerarquía de autoridades de certificación, posiblemente difícil de establecer en la práctica de forma inmediata, pero necesaria a la larga para su buen funcionamiento, el segundo modelo de autocertificación no ofrece en principio dificultades prácticas de implantación, pero, a la larga, puede suponer una anarquía que dificulte su funcionamiento. Pues, en efecto, de no existir una adecuada estructuración (o incluso si ésta existe sólo a nivel interno, pero no alcanza el ámbito internacional), las terceras partes de confianza deberán ofrecer acuerdos con otras terceras partes a fin de formar una red que permita a un usuario comunicarse de forma segura con cualquier usuario de cualquier tercera parte de confianza con la

del sello electrónico–; h) el lugar en que está disponible gratuitamente el certificado electrónico que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra anterior –sin equivalente dentro del anexo I DFE–; i) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado de firma electrónica –sin equivalente dentro del anexo I DFE–, y, j) cuando los datos de creación de firma electrónica relacionados con los datos de validación de la misma se encuentren en un dispositivo cualificado de creación de firma electrónica, una indicación adecuada de este hecho, al menos en una forma apta para el procesamiento automático[512] –sin equivalente dentro del anexo I DFE–.

Por lo demás, la necesidad de cumplir estos requisitos por los certificados cualificados de firma electrónica es reiterada por el artículo 28.1 Reglamento eIDAS, precepto este que aclara, en su apartado segundo, que tales certificados no estarán sujetos a ningún requisito obligatorio que exceda de cuantos se contienen en el anexo I (con el objetivo claro de garantizar su aceptación por los demás Estados miembros), pudiendo contemplar, eso sí, requisitos voluntarios, siempre que no afecten a la interoperabilidad y al reconocimiento de las firmas electrónicas cualificadas[513] (apartado tercero). Este artículo 28 contiene un último apartado en el que establece que la Comisión podrá, mediante actos de ejecución (que seguirán el procedimiento de examen contemplado en el artículo 48.2), establecer números de

---

que su propia tercera parte tenga un acuerdo (sería el tema de los convenios entre autoridades y las certificaciones cruzadas). Todo ello dada la importancia de la interoperabilidad con otras distintas autoridades de certificación y entre autoridades nacionales y extranjeras».

[512] En cambio, recogidos en el anexo I DFE, pero no en el anexo I RIE-SCTE, los siguientes: d) un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado electrónico reconocido; i) los límites del uso del certificado reconocido, si procede, y j) los límites del valor de las transacciones para las que puede utilizarse el certificado reconocido, si procede. No obstante, estas dos últimas condiciones aparecen contempladas también por el Reglamento eIDAS, que hace mención a las mismas al hablar de los requisitos a satisfacer por los PSSIisc cualificados –considerando 37 y artículos 13.2 y 24.2.d) RIE-SCTE–, si bien ya no será necesario que formen parte del contenido necesario del certificado electrónico cualificado, con el consiguiente perjuicio, entiendo, para los terceros que se relacionen con el firmante, que ya no podrán advertir y conocer, al menos tan fácilmente como antes, los límites de uso y de valor de los certificados electrónicos, límites que conllevarán, en su caso, importantes limitaciones a la responsabilidad de los PSSIisc.

[513] Desaparece la necesidad de consentimiento o solicitud del propio firmante como autorización previa para incluir este contenido adicional y no obligatorio en certificados electrónicos cualificados, sí existente en los artículos 8.1e) y 8.2 RDLFE y 11.3 LFE.

referencia de normas relativas a los certificados cualificados de firma electrónica, presumiéndose el cumplimiento de los requisitos contenidos en el anexo I RIE-SCTE cuando el certificado en cuestión se ajuste a tales normas.

Finalmente, conviene aludir al artículo 51 del Reglamento, que establece un elenco de medidas transitorias necesarias para una total adaptación a la nueva normativa comunitaria de los dispositivos seguros de creación de firma electrónica (apartado primero), de los certificados electrónicos reconocidos (apartado segundo) y de los PSSIic que emitan certificados electrónicos reconocidos (apartado tercero), todos ellos determinados con arreglo a la DFE. En concreto, y por lo que aquí interesa, el artículo 51.2 RIE-SCTE dispone expresamente que los certificados electrónicos reconocidos expedidos para las personas físicas conforme a la derogada Directiva se considerarán certificados electrónicos cualificados con arreglo al Reglamento eIDAS hasta que caduquen.

En nuestro país, los certificados electrónicos reconocidos (de firma electrónica –y sólo de firma electrónica–) comenzaron a disciplinarse con el artículo 2.j) RDLFE, que se remitía al artículo 8 para las condiciones a cumplir y al artículo 12 para analizar los requisitos a satisfacer por el PSSIisc[514]. Posteriormente, con la entrada en vigor de la LFE nace el artículo 11.1, que dispone expresamente que serán certificados electrónicos reconocidos aquellos expedidos por un PSSIic «[…] que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes[515] y a la fiabilidad y las garantías de los servicios de certificación que presten»[516]; en concreto, añade un apartado

[514] Sobre esta cuestión, *vid.* PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», cit., pp. 566 a 568.

[515] Artículo 13 LFE.

[516] Ya en el apartado II de la Exposición de Motivos de la LFE se destacaba la existencia de los certificados reconocidos como una clase de certificados electrónicos que cumplen unos requisitos cualificados, subrayando, asimismo, su condición de pieza fundamental para el reconocimiento de la validez de la firma electrónica: «[…] la ley define una clase particular de certificados electrónicos denominados certificados reconocidos, que son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica. Los certificados reconocidos constituyen una pieza fundamental de la llamada firma electrónica reconocida, que se define siguiendo las pautas impuestas en la Directiva 1999/93/CE como la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo

segundo en el que explicita los datos mínimos que deberán contener aquellos certificados electrónicos que quieran tener la condición de reconocidos: a) la indicación de que se expiden como tales –letra a) del anexo I RIE-SCTE y antiguo artículo 8.1.a) RDLFE–; b) el código identificativo único del certificado –letra f) del anexo I RIE-SCTE y antiguo artículo 8.1.b) RDLFE–; c) la identificación del PSSIic reconocido encargado de expedir el certificado electrónico reconocido y su domicilio –letra b) del anexo I RIE-SCTE y antiguo artículo 8.1.c) RDLFE–; d) la firma electrónica avanzada del PSSIic reconocido que expide el certificado electrónico reconocido –letra g) del anexo I RIE-SCTE y antiguo artículo 8.1.d) RDLFE–; e) la identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad[517] o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal[518] –letra b) del anexo I RIE-SCTE y antiguo artículo 8.1.e) RDLFE–; f) los datos de verificación de firma electrónica que correspondan a los datos de creación de la misma que se encuentren bajo el control del firmante –letra d) del anexo I RIE-SCTE y antiguo artículo 8.1.g) RDLFE–; g) el comienzo y el fin del período de validez del certificado electrónico reconocido –letra e) del anexo I RIE-SCTE y antiguo artículo 8.1.h) RDLFE–; h) los límites de uso del certificado electrónico reconocido, caso de que se establezcan –sin equivalente dentro del anexo I RIE-SCTE y antiguo artículo 8.1.i) RDLFE–, e i) los límites del valor de las transacciones para las que puede utilizarse el certificado electrónico reconocido, si se contemplan[519] –sin equivalente dentro del anexo I RIE-

seguro de creación de firma. A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica».

[517] Acertada esta inclusión del DNI como elemento individualizador de la persona física, especialmente útil en aquellos supuestos en que sujetos tengan el mismo nombre y apellidos.

[518] La inclusión de esta referencia a las personas jurídicas, no recogida en el RDLFE, fue consecuencia de que la LFE introdujera la posibilidad de que estas pudieran ser también titulares de firmas electrónicas. Sin embargo, con la entrada en vigor del RIE-SCTE, ha de entenderse derogada esta previsión, que se ve sustituida por la nueva figura del sello electrónico, que tendrá por entidad usuaria a una persona jurídica.

[519] Este requisito se encuentra previsto en el anterior. En cualquier caso, sostiene CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., pp. 82 y 83, «[…] no tiene sentido que ninguna de estas dos menciones sean obligatorias para que el certificado sea reconocido, pues ni la seguridad e integridad del certificado, ni la veracidad o no de su contenido, así como la responsabilidad de la entidad certificadora quedan afectadas. Así, ciertamente el receptor del mensaje firmado y el certificado pueden no conocer tal limitación de responsabilidad si no constan en el propio certificado; pero

SCTE y antiguo artículo 8.1.j) RDLFE–. Asimismo, los certificados electrónicos reconocidos podrán incluir cualquier otra circunstancia o atributo específico del firmante (como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación –artículo 13.3.3º LFE–), siempre que ello suponga un valor adicional en función del fin propio del certificado y así sea solicitado por su titular (artículo 11.3 LFE, que, sin equivalente en la DFE pero sí en el RIE-SCTE –artículo 28.3–, recuerda a los apartados 1.e) y 2 del artículo 8 RDLFE).

Por su parte, el artículo 6.1 del nuevo Anteproyecto de Ley, de manera similar a como hiciera el artículo 11.2.e) LFE, dispone la forma en que se consignará la identidad del titular del certificado (cualificado o no cualificado) de firma electrónica, que será por su nombre, apellidos y número de documento nacional de identidad (que podrá sustituirse por otro código o número identificativo en aquellos casos en que el firmante carezca de él, siempre que le identifique unívocamente), o bien a través de un seudónimo que conste como tal de manera inequívoca; no obstante, el titular de un certificado de firma electrónica con atributo de representante no podrá ser identificado mediante un seudónimo. Además, concluye el precepto (como en su momento concluyera el artículo 11.4 LFE[520]), «[s]i los certificados cualificados admiten una relación de representación incluirán la identidad de la persona física o

este límite le resultará en realidad irrelevante, pues según el artículo 23.1 LFE no le es oponible. En realidad, esto es tanto como decir que el límite no existe en realidad por no haber sido comunicado a los interesados según la forma establecida en el artículo 23.1 LFE. En definitiva, no tiene sentido que un límite que se pueda pretender imponer inútilmente *a posteriori* por el prestador de servicios de certificación, pero que no existe en realidad, desvirtúe la cualidad de reconocido del certificado […]. Evidentemente, una firma reconocida y una firma que no sea reconocida por este motivo tienen el mismo grado de seguridad, con lo que, a nuestro parecer, un tribunal debería concederle el mismo valor, pero no sería ya en virtud del artículo 3.4 LFE, sino por el artículo 3.9 LFE, con la inseguridad jurídica que ello conlleva». Este problema queda subsanado con el RIE-SCTE (artículo 13.2), que no lo incluye como contenido obligatorio de los certificados cualificados de firma electrónica, jugando como elemento de exención de responsabilidad (y siempre que sean superados) sólo cuando el PSSIisc informe debidamente a sus clientes con antelación de estas limitaciones y sean reconocibles por un tercero.

[520] En él se disponía que «[s]i los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13». Antes, y como contenido mínimo del certificado electrónico reconocido, este requisito estaba recogido en el artículo 8.1.f) RDLFE, lo que deja entrever que,

jurídica representada en las formas previstas en el apartado anterior, así como una indicación del documento público[521] que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria, la inscripción de los datos registrales».

### 2.2. Vigencia, suspensión y extinción

Aún en fase de tramitación, el artículo 4 ALSEC dispone que los certificados electrónicos se extinguirán por caducidad a la expiración del período de vigencia. Si bien este período se

---

mientras que antes el certificado electrónico perdía la consideración de reconocido por la no inclusión de esta circunstancia, en la actualidad no tendrá este efecto.

[521] La exigencia de naturaleza pública del documento acreditativo ha de ser valorada positivamente, dado que, desde una perspectiva propiamente jurídica, siempre otorgará mayor seguridad que un simple documento privado. Empero, como en su momento indicara MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 224, «[…] esta exigencia plantea algunas dudas respecto a algunas clases de representación (p. ej., los apoderamientos no generales sino singulares, para determinados actos, cuya inscripción en el Registro Mercantil no es obligatoria, y, por tanto, no constarán necesariamente en documento público) y no soluciona siempre totalmente el problema de la vigencia del poder de representación», que podrá experimentar modificaciones ulteriores; por ende, añade, «[…] para tener conocimiento de estas últimas, […] sería necesaria, en su caso, la inclusión en el certificado de la indicación no ya del documento acreditativo inicial que permite comprobar la existencia inicial del poder sino, en su caso, de los datos registrales que permitan comprobar su vigencia ulterior», razón por la que se incluyó en el artículo 11.4 LFE la obligación de inscripción, caso de ser obligatoria, de los datos registrales, obligación que será heredada por los artículo 6.2 y 7.3 ALSEC. No obstante, en ningún momento se incluye en esta Ley la obligación del PSSIisc de utilizar tal información a efectos de asegurar el mantenimiento de la vigencia del poder contenido en el certificado electrónico en los artículos 11.4, 12 y 13 LFE –si bien sí se permite al amparo del apartado III de la Exposición de Motivos y del artículo 19.1, infiriéndose indirectamente de los artículos 8.1.g) y 23.2 LFE, siempre que el representado tenga conocimiento de la existencia del certificado electrónico, conocimiento no exigido, a diferencia de otros de la época, por el ordenamiento jurídico español–; en cambio, esta obligación sí parece deducirse ahora del artículo 7.3 ALSEC cuando dispone que «[e]n el caso de certificados cualificados de sello electrónico y de firma electrónica con atributo de representante, los prestadores de servicios de confianza comprobarán, además de los datos señalados en los apartados anteriores, los datos relativos a la constitución y personalidad jurídica y a la persona o entidad representada, respectivamente, así como la extensión *y vigencia* de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible. Esta comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos» (la cursiva es propia).

fija en un máximo de cinco años para los certificados electrónicos que sean cualificados, advierte que se especificará con precisión atendiendo a las características y a la tecnología empleada para generar los datos de creación de firma electrónica, heredando la previsión instaurada, como veremos, por el artículo 8.2 LFE. Sin embargo, mientras que la LFE la contempla como una previsión general que afecta a todo tipo de certificados electrónicos, el ALSEC la establece únicamente para delimitar el plazo de duración de certificados electrónicos cualificados.

En cualquier caso, dada la relevancia que para terceros tiene la extinción de certificados electrónicos por finalización del período de vigencia, el anexo I del RIE-SCTE, entre el contenido obligatorio de los certificados electrónicos cualificados, incluye un apartado e) en el que exige que se hagan constar «los datos relativos al inicio y final del período de validez del certificado», precisamente al objeto de que esa circunstancia pueda ser conocida por quienes van a confiar en el mismo. Esta previsión tiene importancia porque, en el caso del tercero usuario, se establece una obligación, o cuanto menos una carga, en el artículo 14.1.e) ALSEC, en virtud de la cual «[e]l prestador de servicios electrónicos de confianza no será responsable de los daños y perjuicios ocasionados a la persona a la que ha prestado sus servicios o a terceros de buena fe[522], si la citada persona incurre en alguno de los supuestos previstos en el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014 o en los siguientes: e) utilizar los datos de creación de firma […] cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de confianza le notifique la extinción o suspensión de su vigencia».

Por lo que respecta a la posible extinción de la vigencia de certificados de firma electrónica, el artículo 28.4 RIE-SCTE regula exclusivamente aquellos que sean cualificados[523], afirmando

[522] Esta redacción resulta ciertamente confusa, ya que no queda del todo claro si los supuestos que se describen seguidamente afectan a la persona a la que el PSSIisc ha prestado sus SSIisc (firmante) o a terceros de buena fe (terceros que confían), habiéndolo de deducir como resultado de la lógica y de la interpretación.

[523] Pese a que en el precepto se habla de revocación, entendemos más adecuado hablar de extinción de la vigencia, ya que la revocación parece hacer alusión más bien a aquellos supuestos en que la validez del certificado electrónico se deja sin efecto (posición activa) antes del momento previsto, mientras que la extinción de la vigencia incluiría también el supuesto en que esta se produce por caducidad o expiración del período de validez del certificado electrónico (posición pasiva).

que, en el supuesto en que sean revocados tras su activación inicial[524], perderán su validez de manera permanente desde el momento preciso en que aquella se produzca, sin que puedan, bajo ninguna circunstancia, volver a recuperar su estado inicial de vigencia. Por su parte, el recién elaborado artículo 5 ALSEC incorporaría una serie supuestos (unos de naturaleza interna, otros externa) que motivarían la extinción de la vigencia de certificados electrónicos por revocación, y lo hace introduciendo una relevante diferencia respecto del Reglamento, y es que no restringe esta cuestión a los certificados electrónicos cualificados, sino que amplía el mínimo marcado a nivel comunitario también a aquellos otros que no lo son; en concreto, y por lo que respecta a la firma electrónica, los PSSIisc procederán como se indica cuando acaezca alguna de las siguientes circunstancias: a) solicitud (entendemos que discrecional o *ad nutum*, sin necesidad de causa justificativa adicional[525]) formulada por el firmante, la persona física o jurídica representada por este[526] o un tercero autorizado[527]; b) violación o puesta

[524] Más adecuado sería decir, tras la explicación contenida en la nota anterior, *en el supuesto en que se extinga la vigencia tras su activación inicial.*

[525] *Ibid.*, p. 173.

[526] De la lectura conjunta de ambas normas (RIE-SCTE y ALSEC), no termina de quedar del todo claro si se permite la posibilidad de que el firmante (necesariamente persona física) pueda actuar, no sólo en representación de una persona jurídica, sino también de una persona física. Y es que, si bien es cierto que del concepto de firmante que ofrece el Reglamento (el ALSEC no ofrece ninguna definición al respecto) sólo se infiere que quien firma ha de ser una persona física, no lo es menos que una de las finalidades básicas de la firma electrónica (al igual que sucede con la firma manuscrita) es la identificación electrónica del firmante, entendiéndose por tal el proceso de utilizar los datos de identificación de una persona (física o jurídica) en formato electrónico que representan de manera única a una persona física (firma electrónica) o jurídica (sello electrónico) o a una persona física (firma electrónica) que representa a una persona jurídica. Hasta aquí, fácilmente podríamos concluir que legalmente se excluye la posibilidad de que el firmante represente a otra persona física; sin embargo, del análisis complementario del artículo 5.1.a) ALSEC podemos sostener una postura ciertamente más amplia, que incluye la capacidad del firmante de representar por medio de la plasmación de su firma electrónica no sólo a una persona jurídica (algo que parece más que claro) sino también a una persona física, habida cuenta de que «[…] *la persona física* o jurídica representada por este (firmante)» también podrá realizar la solicitud de suspensión de certificados electrónicos, resolviéndose, por tanto, de modo indirecto, la duda planteada (la cursiva y el paréntesis que se hallan dentro del entrecomillado son propios).

[527] Esta previsión («[…] la persona física o jurídica representada por este o un tercero autorizado») nos sitúa ante los conocidos como *certificados de atributos*, en concreto, ante aquellos que incluyen como atributo un poder de representación en virtud del cual se autoriza al titular de un certificado electrónico a actuar (es decir, a firmar electrónicamente) en nombre de otra persona; sin embargo, al igual que sucedía con el RDLFE y con la LFE, el nuevo Anteproyecto sigue sin pronunciarse sobre si esta actuación para la que se legitima a las personas

en peligro del secreto de los datos de creación de firma electrónica o del PSSIisc[528] o utilización de dichos datos por un tercero[529]; c) resolución judicial o administrativa que ordene la suspensión; d) fallecimiento o incapacidad sobrevenida, total o parcial, del firmante[530]; e)

representadas es simplemente una facultad o, más bien, una carga. Los certificados de atributos permiten incluir otros datos de interés (ello determina que el firmante tenga, en su caso, un certificado de identidad y podrá tener varios certificados de atributos –por ejemplo, por ser apoderado de varias personas–), como la edad, la capacidad para contratar o apoderamientos dentro de una empresa, entre otros. Para un estudio más profundo de los certificados de atributos, *vid.* DÍAZ MORENO, A., «Certificados de clave pública y entidades de certificación», en PERALES SANZ, J. L. (coord.) *La seguridad jurídica en las transacciones electrónicas: seminario organizado por el Consejo General del Notariado en el UIMP*, Madrid, Civitas, 2002, pp. 95 y 96; GONZÁLEZ-ECHENIQUE CASTELLANOS DE UBAO, L., «Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre firma electrónica», en DE ROS CEREZO, R. M./CENDOYA MÉNDEZ DE VIGO, J. M. (coords.) *Derecho de Internet : la contratación electrónica y firma digital*, 2000, p. 232; MARTÍNEZ NADAL, A., «Problemática jurídica de los certificados de atributos en el comercio electrónico. En especial, su discordancia con el Registro Mercantil», en ORDUÑA MORENO, F. J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, pp. 659 a 709; RIBAGORDA GARNACHO, A., «Sistema de certificación: la firma y el certificado digital», en FERNÁNDEZ ORDOÑEZ, M./CREMADES GARCÍA, J./ILLESCAS ORTIZ, R. (coords.) *Régimen jurídico de Internet*, Las Rozas, Wolters Kluwer, 2001, pp. 1324 a 1329.

[528] La redacción de esta causa resulta ciertamente confusa, ya que no se indica qué violación o puesta en peligro debe experimentar concretamente el PSSIisc. No obstante, de la lectura del prácticamente idéntico (a excepción de los cambios propios de la ampliación de los servicios de confianza introducidos) artículo 8.1.c) LFE, cabe considerar que, en lo que interesa a este estudio, se estaría refiriendo a la violación o puesta en peligro de los datos de creación de firma electrónica, no sólo del firmante, sino también del PSSIisc.

[529] Nada se dice expresamente acerca de si la persona afectada por esta violación o puesta en peligro es la encargada de proceder a solicitar la extinción anticipada del certificado electrónico. *A priori*, cabría entender que sí, pues así se infiere de la lectura conjunta de este precepto con el artículo 14.1.d) ALSEC, que contempla como obligación del firmante la de «[…] solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma […] o, en su caso, de los medios que den acceso a ellos». Esta obligación –siempre sobre la base del artículo 5.1.a) ALSEC– se extendería igualmente, en aquellos supuestos en que el certificado electrónico recoja una relación de representación por el firmante, a la persona representada –artículo 5.1.e) ALSEC–. Además, cabe también la posibilidad de que el propio PSSIisc tenga noticia de esta circunstancia, en cuyo caso cabría entender que tendría la obligación de extinguir, ahora directamente, el certificado electrónico afectado.

[530] La duda que esta causa sigue planteando es la de la persona que ha de asumir la carga de solicitar la extinción anticipada del certificado electrónico en el caso de fallecimiento del firmante (no tanto en el de incapacidad sobrevenida, total o parcial, en el que cabe entender que, entre las obligaciones de un tutor diligente, se incluirá la de solicitar la extinción del certificado electrónico, siempre que tenga conocimiento de su existencia), ya que

terminación de la representación en los certificados electrónicos con atributo de representante, estando obligados tanto el representante como la persona o entidad representada a solicitar, a tal fin, la revocación de la vigencia de certificado electrónico en cuanto se produzca la modificación o extinción de la relación de representación[531]; f) cese en la actividad del PSSIisc, salvo que la gestión de los certificados electrónicos por él expedidos sea transferida a otro PSSIisc, en cuyo caso, se entiende, el certificado electrónico no se extinguirá sino hasta que concluya el período inicial de validez estipulado; g) descubrimiento de falsedad o inexactitud en los datos aportados para la expedición del certificado electrónico, como las relativas al cargo, y h) cualquier otra causa lícita prevista en la declaración de prácticas del SSIisc[532].

Desaparecería con la futura entrada en vigor del presente Anteproyecto una importante previsión contenida en la LFE (artículo 8.3), como es la relativa al momento a partir del cual la extinción de la vigencia del certificado electrónico surtirá efectos y a quiénes afectarán estos efectos. Así las cosas, cabría entender que, al igual que entonces, estos efectos tendrán lugar frente a terceros y lo tendrán desde que se produzca el hecho, en los supuestos de expiración de su período de validez (supuesto de eficacia inmediata), y desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados electrónicos expedidos por el PSSIisc, en los demás casos (supuestos de eficacia diferida o condicionada).

---

no siempre el PSSIisc tiene conocimiento cierto y rápido de tales hechos. Por lo demás, desaparece, no entendemos bien por qué, el supuesto de extinción de la vigencia del certificado electrónico por fallecimiento; extinción de la personalidad; incapacidad sobrevenida, total o parcial, o disolución del representado, persona física (en el caso de fallecimiento) o jurídica (en todos los demás supuestos mencionados).

[531] A diferencia de lo que sucedía con el RDLFE y con la LFE, ahora sí se resuelve de manera expresa quiénes son las personas que tienen la obligación de solicitar la extinción de la vigencia del certificado electrónico cuando concurra esta circunstancia, cuestión que permitirá resolver, en su caso, las posibles discrepancias entre la apariencia derivada del Registro Mercantil y la apariencia derivada del correspondiente certificado de atributos.

[532] Lo que deja entrever que nos hallamos ante un verdadero listado *numerus apertus*, por poder introducir en la declaración de prácticas de servicios de confianza del PSSIisc toda posible causa de extinción (también de suspensión, al amparo del artículo 5.2 ALSEC) de la vigencia del certificado electrónico que no se encuentre en el elenco antes enumerado (FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., pp. 67 y 70). Por lo demás, tampoco aquí se indican los sujetos que estarían legitimados para llevar a cabo la solicitud de extinción de la vigencia del certificado electrónico.

También debemos ocuparnos en este apartado de la suspensión. De acuerdo con el considerando 53 RIE-SCTE, podemos decir que por suspensión se entiende aquella práctica operada por los PSSIisc en una serie de Estados miembros que, distinta de la extinción (como sabemos, de carácter definitivo), conlleva la pérdida *temporal* de la validez de un certificado electrónico. La suspensión indica, generalmente, que un certificado electrónico es sospechoso por alguna circunstancia, siendo adecuada, cuando esta tiene lugar, la especificación del tiempo en el que comienza y en el que finaliza (finalización que puede producirse anticipadamente); transcurrido este período, se deberá optar, bien por seguir considerando el certificado electrónico válido y operativo, bien por revocarlo de forma definitiva[533].

Si bien es cierto que la normativa no impone su uso, sí que deben establecerse normas de transparencia en aquellos casos en que se habilite esta opción. A tal efecto, el artículo 28 del Reglamento eIDAS dispone, esta vez en su apartado quinto, que los Estados miembros que así lo estimen conveniente podrán fijar normas nacionales sobre suspensión temporal, siempre bajo dos presupuestos elementales: uno, la suspensión temporal, de producirse, hace que el certificado electrónico cualificado pierda su validez durante el tiempo que dure la suspensión; dos, el período de suspensión del certificado electrónico ha de indicarse con claridad en la base de datos de certificados y el estado de suspensión será visible, mientras dure, a partir del servicio que proporcione información sobre el estado del certificado.

Sobre la base de esta previsión normativa, el artículo 5.2 ALSEC persigue regular la posibilidad que tienen los PSSIisc de suspender la vigencia de certificados electrónicos, incluyendo también (como ya sucediera con la extinción) tanto a los certificados electrónicos cualificados como a los que no lo sean. Tampoco, al igual que con la extinción y como ya sucediera en el RDLFE y en la LFE, se regula de modo explícito (aun cuando sí puede deducirse de la regulación de las distintas causas que pueden motivarla) la cuestión de la iniciativa de la suspensión, que puede ser también a solicitud del titular, por decisión del propio PSSIisc o a instancia de un tercero distinto del firmante[534]. En concreto, dispone que, por lo que respecta a la firma electrónica, la misma podrá ampararse en cualquiera de los supuestos previstos en

[533] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., pp. 194 y 198.

[534] Bien es cierto que el artículo 9.4 RDLFE no establecía la legitimación de la entidad certificadora para suspender un certificado electrónico a iniciativa propia. En cambio, el artículo 9.1 LFE contempla implícitamente esta posibilidad en los apartados c) y d), además de proporcionar una regulación más detallada de la legitimación de terceros distintos del titular en el apartado a).

las letras a), c) y h) del artículo 5.1 inmediatamente anterior, capaces también, como hemos visto, de propiciar la revocación; a ellos se añadiría un cuarto supuesto, relativo a aquellos casos de duda sobre la concurrencia de las circunstancias previstas en las letras b) y g), también del artículo 51.1, siempre que sus declaraciones de prácticas de certificación prevean la posibilidad de suspender los certificados electrónicos. Además, como ya previera en su momento el artículo 10.2, *in fine*, LFE, de no ser levantada la suspensión por el PSSIisc del certificado electrónico, cualificado y no cualificado, una vez transcurrido su respectivo plazo de duración (cuyo máximo legal no se establece[535]), se producirá la extinción automática de su validez (artículo 51.3, *in fine*, ALSEC). Al igual que sucediera con la extinción definitiva de la vigencia del certificado electrónico, no se regula, tampoco aquí, el momento a partir del cual la suspensión surtirá efectos, habiendo de entender, tras una interpretación extensiva del contenido de la normativa anterior (artículo 9.2 LFE), que este momento será el de la inclusión en el servicio de consulta sobre el estado de validez o extinción de los certificados electrónicos expedidos por el PSSIisc, servicio que será obligatorio de acuerdo con el artículo 11.2.b) ALSEC; consecuencia de esta interpretación, unida a la prevista para la extinción de la vigencia, también cabría entender que la suspensión surtirá efectos únicamente frente a terceros.

Sin embargo, ni para la extinción ni para la suspensión de la vigencia del certificado electrónico se establece el momento en el que el PSSIisc tendrá que hacerla constar en el servicio de consulta. De nuevo, debemos acudir a la LFE, concretamente a su artículo 10.1, que dispone que esta circunstancia habrá de ser recogida inmediatamente, de manera clara e indubitada, «[…] en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia»; de acoger esta previsión, y como ya hiciera el artículo 22.3 LFE, sería necesario introducir paralelamente un nuevo supuesto en materia de responsabilidad del PSSIisc que lo declarara responsable por los perjuicios causados al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta de la extinción o suspensión de la vigencia del certificado electrónico afectado.

[535] Quizás, la razón se deba a que la suspensión dependerá del tipo de certificado electrónico y de las circunstancias que originan la suspensión. En todo caso, convendría que estuviese previsto en la declaración de prácticas de certificación del PSSIisc (artículo 12 ALSEC), a fin de evitar supuestos de suspensiones indefinidas; así lo prevé (y así lo debería prever el ALSEC) el artículo 10.2, *in fine*, LFE, que establece que el PSSIic deberá indicar la duración máxima (subjetiva, ya que, como decimos, no se indica) del certificado electrónico, transcurrida la cual se extinguirá su vigencia si no se levanta la suspensión.

Tampoco se recoge si la extinción o suspensión conllevarán efectos retroactivos (aspecto este que tendría que negarse, si acogemos el criterio establecido por el artículo 10.3 LFE) ni hasta cuándo se mantendrá accesible en el servicio de consulta (que será, al menos, hasta la fecha en que hubiera finalizado su período inicial de validez, si nos atenemos a lo que dispone el artículo 10.4 LFE). En relación con este último aspecto, nace el artículo 24.2.h) RIE-SCTE, que establece la obligación de todo PSSIisc cualificado de registrar y mantener accesible «[…] durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos»; de esta previsión nacería el, en fase de tramitación, artículo 11.3.a) ALSEC, que dispone que los PSSIisc cualificados habrán de conservar la información relativa a los SSIisc cualificados prestados de acuerdo con el precitado artículo del Reglamento eIDAS durante un tiempo de quince años.

Por último, cuando se trate de certificados electrónicos cualificados, de manera previa o simultánea a la indicación de su extinción o suspensión en el servicio de consulta sobre el estado de validez de certificados por él expedidos –artículo 11.2.b) ALSEC–, el PSSIisc cualificado informará al firmante acerca de esta circunstancia, especificando los motivos y la fecha y hora en que aquel quedará sin efecto, ya sea permanentemente –extinción– o tan sólo de manera temporal –suspensión– (artículo 51.3, *ab initio*, ALSEC).

Antes de la entrada en vigor del Reglamento eIDAS, la DFE prácticamente no se refería a la cuestión de la vigencia, suspensión y extinción de certificados electrónicos, que sí sería abordada de manera específica en nuestro país en los artículos 8 a 10 LFE (antes, artículo 9 RDLFE). Al igual que el ALSEC, la Ley (también el Real Decreto-ley) aborda la extinción de la vigencia y la suspensión de los certificados electrónicos, sin excluir a aquellos que no sean cualificados.

De acuerdo con el primero de los preceptos, el período máximo de validez de los certificados electrónicos reconocidos quedaba fijado también en cinco años, contados, a falta de

indicación expresa al respecto, desde la fecha de su expedición[536] (artículo 8.2 LFE)[537]; en concreto, en lugar de establecer un plazo temporal concreto de forma general, la Ley opta por la exigencia genérica de adecuación del período de validez a las características y tecnología empleada para la generación de los datos de creación de firma electrónica, estableciendo

[536] CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 73.

[537] En el RDLFE, al igual que en la LFE antes de la modificación operada por el apartado 2 de la D. F. 6 LGT, el período máximo de cuatro años para los certificados electrónicos reconocidos (inferior, por tanto, al de cinco fijado posteriormente en la LFE y en el ALSEC) fue criticado por VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., p. 153, que ya por entonces lo consideraba excesivo teniendo en cuenta el rápido avance de los progresos tecnológicos, rápido avance del que se hace eco también FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 65, a la hora de justificar la limitación de plazos. Lo cierto es que, como señala MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 167, «[…] 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: a) para controlar las oportunidades de criptanálisis, porque, en efecto, el riesgo de ruptura del par de claves es mayor por la mayor exposición frente a terceros, que tienen más tiempo y más datos para consumar el ataque: cuanto más tiempo se use un par de claves, mayores son las posibilidades de ruptura; por contra, cambiar el par de claves limita el daño que cualquier ruptura de la seguridad de un par de claves, a través del criptanálisis, o de otros medios, podría causar, b) o, simplemente, para reducir el período de vulnerabilidad en que las claves podrían resultar comprometidas (posibilidad de robo, extravío, revelación de la clave privada a terceros, etc.) y c) así como para evitar el desfase técnico, la degradación de la calidad de la clave por el simple paso del tiempo, que, junto con los avances técnicos, pueden provocar que claves inicialmente válidas y fiables en el momento de su generación, devengan inseguras y poco fiables un tiempo más o menos breve después (así, p. ej., puede producirse un gran descubrimiento y entonces los algoritmos en que las claves del titular del certificado y de la entidad de certificación están basados ya no son seguros)». En cualquier caso, adiciona, «[d]entro de los límites legales (si es que existen y afectan al certificado en cuestión), la duración del período de validez del certificado es una cuestión política de la entidad de certificación y que implica y afecta a los diversos sujetos intervinientes. Los valores usados varían de varios meses a varios años; períodos de vigencia de uno a tres años son habituales para certificados de titulares que son destinatarios finales, es decir, que no vayan a actuar como entidad de certificación. En cambio, para los certificados de entidades certificadoras, pueden resultar más adecuados períodos más largos, porque sus cambios de clave […] son más complejos. La duración puede ser la misma para todos los certificados de una misma entidad, o puede ser diferente en función de la naturaleza y de la condición del usuario (p. ej., en el caso de certificados emitidos por una empresa para sus empleados, los certificados destinados a empleados eventuales tendrán un período de validez más breve que los destinados a empleados fijos)». En torno a las consecuencias de la temporalidad de los certificados electrónicos, *vid.* LAFUENTE SUÁREZ, M., «Análisis de la Ley 59/2003, de firma electrónica, tras dos años de vigencia: problemas no resueltos en torno a los certificados de firma electrónica», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 11, 2006, p. 17.

después, y sólo para el caso de certificados electrónicos reconocidos, un plazo máximo legal concreto no superior a cinco años[538]. Además, se establecen como causas de extinción definitiva de la vigencia de un certificado electrónico (cualificado y no cualificado) prácticamente las mismas que las recogidas en el artículo 5.1 ALSEC[539] (artículo 8.1 LFE): a) expiración del período de validez antes aludido y que figura en el certificado –antiguo artículo 9.1.a) RDLFE y artículo 4 ALSEC–; b) revocación[540] por el firmante o titular del certificado[541], la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica[542] –antiguo artículo 9.1.b) RDLFE y artículo

[538] En concreto, dispone este apartado, «[e]l período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma. En el caso de los certificados reconocidos este período no podrá ser superior a cinco años»; esta inclusión resulta especialmente necesaria si tenemos en cuenta que el artículo 8.3 LFE configura la extinción como una causa de eficacia inmediata, no condicionada a publicación posterior alguna. Tampoco en el RDLFE existía un período máximo de validez legal (sí técnica) de los certificados electrónicos no reconocidos; así se desprende del artículo 8.1.h) RDLFE, que, relativo a la inclusión en el contenido del certificado electrónico del período de validez, resulta de aplicación únicamente a los que son reconocidos.

[539] No obstante, como ya indicamos anteriormente, pese a la larga enumeración contenida en este primer apartado, las causas de extinción de la vigencia de un certificado electrónico pueden agruparse en dos grandes categorías: invalidez del certificado por finalización del plazo de vigencia previsto en el mismo e invalidez anticipada (revocación) por causas no previstas inicialmente (MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 165).

[540] Inadecuación del término *revocación* empleado tanto por el RDLFE como por la LFE, ya que quien revoca el certificado electrónico no es el firmante o signatario, la persona física o jurídica representada por este, un tercero autorizado o la persona física solicitante de un certificado de persona jurídica, sino la entidad certificadora que lo ha emitido, previa solicitud, eso sí, de tales sujetos. Como hemos podido ver, este defecto se vería solventado por el ALSEC, si bien en parte, ya que lo adecuado, más que de *solicitud*, sería hablar de *solicitud de revocación*.

[541] Antes, el firmante podía ser persona física o jurídica y, a su vez, podía representar a una persona física o jurídica. Sin embargo, como hemos visto, con la aparición en el nuevo RIE-SCTE del sello electrónico, desaparece la posibilidad de que el firmante pueda ser una persona jurídica, si bien se mantiene la posibilidad –así parece deducirse del artículo 5.1.a) ALSEC, no tanto del Reglamento eIDAS– de que este represente a una persona física o a una persona jurídica.

[542] Pese a que esta previsión queda derogada con la RIE-SCTE, es preciso hacer constar que nada se indica en este punto respecto de la posible obligatoriedad o, por el contrario, mera facultad de estos representantes de personas jurídicas de solicitar la extinción anticipada de la vigencia del certificado electrónico. No obstante, la cuestión queda resuelta, al menos parcialmente, en el apartado correspondiente a la responsabilidad del PSSIic, concretamente, en el artículo 23.3 LFE, que establece que «[c]uando el firmante sea una persona jurídica, el

5.1.a) ALSEC–; c) violación o puesta en peligro de los datos de creación de firma electrónica del firmante o del PSSIic o utilización indebida de dichos datos por un tercero[543] –antiguo artículo 9.1.d) RDLFE[544] y artículo 5.1.b) ALSEC–; d) resolución judicial o administrativa que así lo ordene –antiguo artículo 9.1.e) RDLFE y artículo 5.1.c) ALSEC–; e) fallecimiento o extinción de la personalidad jurídica del firmante, fallecimiento o extinción de la personalidad jurídica del representado, incapacidad sobrevenida (total o parcial) del firmante o de su representado[545], terminación de la representación, disolución de la persona jurídica representada[546] o alteración de las condiciones de custodia o uso de los datos de creación de firma

solicitante del certificado electrónico asumirá las obligaciones indicadas en el apartado 1», entre las cuales se encuentra –artículo 23.1.b) LFE– la «[…] comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico».

[543] Al elenco de presuntamente legitimados para solicitar la extinción por esta causa, ya indicados en el apartado correspondiente del ALSEC, cabría incluir aquí al solicitante del certificado electrónico en el supuesto de certificados electrónicos de persona jurídica (artículo 23.3 LFE).

[544] Se amplía el número de causas respecto al artículo 9.1.d) RDLFE, si bien todas ellas tienen un fundamento común: la violación o puesta en peligro de los datos de creación de firma electrónica del firmante o del PSSIic. Además, en este último precepto, pese a aparecer el sujeto responsable de la utilización indebida («un tercero»), no se hacía constar el objeto de esa utilización indebida, que queda claro con la incorporación de la LFE: «dichos datos», en alusión a los datos de creación de firma electrónica del firmante o del PSSIic. Por lo demás, desaparece en la LFE la posible causa, contenida en el artículo 9.1.c) RDLFE, relativa a la «[p]érdida o inutilización por daños del soporte del certificado», posiblemente por las dudas e incógnitas que su contenido planteaba.

[545] Sin embargo, paralelamente no se incluyen, ni en el RDLFE ni en la LFE, supuestos de inhabilitación o modificación parcial de las facultades del representado que tenga la condición de persona jurídica.

[546] Introduce como posible causa de extinción de la vigencia de certificados electrónicos la extinción de la personalidad jurídica del firmante, la extinción de la personalidad jurídica del representado y la disolución de la persona jurídica representada, pero no la disolución de la persona jurídica firmante.

electrónica que estén reflejadas en los certificados electrónicos expedidos a una persona jurídica –antiguo artículo 9.1.f) RDLFE[547] y artículo 5.1.d) y e) ALSEC[548]–; f) cese en la actividad del PSSIic, salvo que, previo consentimiento expreso por parte del firmante, la gestión de los certificados de firma electrónica por él expedidos sean transferidos a otro PSSIic –antiguo artículo 9.1.g) RDLFE y artículo 5.1.f) ALSEC–; g) alteración de los datos aportados para la obtención del certificado electrónico o modificación de las circunstancias verificadas para la expedición del mismo, como las relativas al cargo o a las facultades de representación, de manera que este no fuera conforme a la realidad –sin equivalente en la RDLFE[549] y artículo 5.1.g) ALSEC–, y h) cualquier otra causa lícita prevista en la declaración de prácticas de certificación –artículo 5.1.h) ALSEC–. Además, añade (no así el ALSEC, sí el RDLFE –artículo 9.2–), esta extinción de la vigencia del certificado electrónico surtirá efectos frente a terceros, en el supuesto de la letra a), desde que se produzca esta circunstancia[550], y, en el resto de supuestos de revocación de las letras b) a h), desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del PSSIic (artículo 8.3 LFE[551]).

---

[547] La LFE introduce, no obstante, algunas modificaciones con respecto al RDLFE, como la incorporación del término *firmante*, la inclusión de la disolución de la persona representada y la contemplación de la persona jurídica como posible titular de certificados electrónicos.

[548] No incorpora el Anteproyecto, como sí hacía la LFE, el fallecimiento o la incapacidad sobrevenida del representado; tampoco la disolución de la persona jurídica representada. Imagino que todas ellas podrán seguir aludiéndose como causas de extinción de la vigencia de certificados electrónicos expedidos a favor del firmante al amparo de la letra h) del artículo 5.1 ALSEC.

[549] Esta causa se introduce suplantando, aun cuando puede llegar a coincidir, a la contenida en el artículo 9.1.h) RDLFE, sobre inexactitudes graves en los datos aportados por el signatario para la obtención del certificado electrónico, que nos sitúa, por tanto, ante la existencia de certificados electrónicos inexactos, falsos o incorrectos.

[550] En el RDLFE se incluía también, como causa de extinción que produce efectos inmediatos frente a terceros, el cese de actividad del PSSIic, que pasa con la LFE a incluirse dentro de las causas con eficacia diferida o condicionada. Parece adecuado dejar en el primer grupo únicamente la causa consistente en la extinción del período de validez por ser la única que puede y debe ser conocida fácilmente por el tercero usuario sin necesidad de realizar búsquedas excesivamente complejas.

[551] Como podemos observar, este artículo 8.3 LFE resuelve tan sólo la eficacia de la extinción de la vigencia de un certificado electrónico frente a terceros, pero no entre el titular del certificado y el PSSIic. Tampoco regula

Por su parte, la suspensión queda reflejada en el artículo 9 LFE (antiguo artículo 9.4 RDLFE), que deberá practicarse cuando concurra alguna de las causas contenidas en los apartados a) –equivalente con el artículo 8.1.b) LFE–, b) –equivalente con el artículo 8.1.d) LFE– y d) –equivalente con el artículo 8.1.h) LFE– del artículo 9.1 LFE, así como por la existencia en el PSSIisc de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados de firma electrónica contemplados en las letras c) y g) del artículo 8.1 LFE –artículo 9.1.c) LFE–. Esta posible suspensión surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados electrónicos del PSSIic. Todas ellas se corresponden íntegramente con las recogidas en el texto del artículo 5.2 ALSEC, que añade la necesidad de que, con respecto a la última de las causas señaladas, las declaraciones de prácticas de certificación prevean la posibilidad de suspender los certificados electrónicos.

Finalmente, el artículo 10 LFE contiene una serie de disposiciones comunes a la extinción y a la suspensión de la vigencia de certificados electrónicos (algunas de las cuales ya han sido apuntadas), haciéndolas extensibles tanto a los certificados electrónicos reconocidos como a los que no lo son y diferenciándose, por tanto, de su equivalente artículo 5.3 ALSEC, que, además de ser menos explícito o detallado, únicamente impone su contenido a los certificados electrónicos cualificados. De acuerdo con este precepto, será obligatorio para el PSSIic hacer constar inmediatamente, de manera clara e indubitada, la extinción o suspensión arriba descritas en el servicio de consulta sobre la vigencia de los certificados electrónicos tan pronto como tenga conocimiento fundado de cualquiera de los hechos determinantes de las mismas[552] (previsión temporal esta no incluida en el precepto del ALSEC)[553]. Además, informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o

el procedimiento de extinción ni resuelve las importantes implicaciones en materia de responsabilidad que pueden derivarse de las distintas fases (por ejemplo, en el supuesto de revocación anticipada de la vigencia del certificado electrónico por pérdida de la clave privada, acaecimiento de la pérdida en sí, conocimiento de esta circunstancia por quien sea el titular, petición de revocación del certificado por el titular y dirigida a la entidad emisora, recepción de la petición, confirmación de la misma y decisión efectiva de revocar el certificado) que se suceden hasta que se produce la extinción anticipada del certificado electrónico (*Ibid.*, p. 191).

[552] De lo contrario, incurrirá en el supuesto de responsabilidad previsto en el artículo 22.3 LFE.

[553] En consecuencia, el PSSIisc no sólo actuará a iniciativa y previa petición del firmante titular del certificado electrónico, sino también a iniciativa de terceros o cuando, de cualquier otro modo, «[…] tenga conocimiento

suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y hora en que este quedará sin efecto. En los casos de suspensión, indicará su duración máxima (nada dice el ALSEC al respecto), extinguiéndose la vigencia del certificado electrónico si, transcurrido dicho plazo, no se hubiera levantado la suspensión. Para concluir, incorpora dos previsiones que posteriormente, como hemos visto, desaparecerán en el Anteproyecto de Ley: una primera, que aclara que la extinción o suspensión de la vigencia del certificado electrónico no tendrá efectos retroactivos, y una segunda, que exige que esta circunstancia se mantenga accesible en el servicio de consulta al menos hasta la fecha en que hubiera finalizado su período de validez inicial[554].

### 3. Datos y dispositivos de firma electrónica

Esenciales en la conformación de la infraestructura de clave pública a la que hacíamos referencia en líneas anteriores son, además de los certificados electrónicos, los datos y dispositivos de firma electrónica. Ambos permitirán el desarrollo de aquellos aspectos que podríamos considerar más importantes, por ser imprescindibles para la implementación de este

---

fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia» (artículo 10.1, *in fine*, LFE).

[554] Así, si la validez para los certificados electrónicos reconocidos tiene un período máximo de cinco años desde la fecha en que se expide (artículo 8.2 LFE) y se expide, por ejemplo, el 1 de enero de 2014, eso quiere decir que su período inicial de vigencia se extenderá hasta el 1 de enero de 2019; hasta ese día, tiene que constar la extinción de la vigencia del certificado electrónico reconocido en el servicio de consulta, fecha esta que coincidirá con el supuesto del artículo 8.1.a) LFE. Si el certificado electrónico no es reconocido, no tendrá un período máximo inicial de validez, pudiendo durar, por ejemplo, diez años, hasta el 1 de enero de 2024, y debiendo constar la extinción de la vigencia del certificado electrónico no reconocido en el servicio de consulta hasta ese mismo día, fecha esta que coincidirá con el supuesto del artículo 8.1.a) LFE. En las demás causas del artículo 8.1 LFE, el certificado electrónico (reconocido o no) puede extinguirse antes, pero deberá constar la causa de extinción hasta el 1 de enero de 2019 o hasta el 1 de enero de 2014, respectivamente. Con respecto a la suspensión, no existe un período máximo de duración, pero sí se establece que, si transcurrido el plazo previamente establecido, no se ha levantado la misma, el certificado electrónico extinguirá su validez (artículo 10.2 LFE). De este modo, si un certificado electrónico reconocido extingue su vigencia a los cinco años desde la fecha en que se expide (artículo 8.2 LFE) y se expide el 1 de enero de 2014, eso quiere decir que su período inicial de validez se extenderá hasta el 1 de enero de 2019; hasta ese día tiene que constar la suspensión de la vigencia del certificado electrónico en el servicio de consulta; si el certificado electrónico no es reconocido, no tendrá un período máximo inicial de validez, pudiendo durar, por ejemplo, diez años, hasta el 1 de enero de 2024, y debiendo constar la suspensión de la vigencia del certificado electrónico no reconocido en el servicio de consulta hasta ese mismo día.

esencial SSIisc: estamos haciendo referencia a los elementos técnicos que permitirán la creación, primero, y la verificación o validación, después, de firmas electrónicas. De todo ello nos vamos a ocupar en el presente apartado.

### 3.1. Datos y dispositivos de creación

El apartado 13) del artículo 3 RIE-SCTE aporta una definición de los datos de creación de firma electrónica como los datos únicos que utiliza el firmante para crear una firma electrónica. Son, por tanto, datos que, incorporados a un chip electrónico, banda magnética o disco duro de un ordenador, permiten generar la firma electrónica, evitando razonablemente (con base en criterios matemáticos o estadísticos) su duplicación[555].

Si observamos el Reglamento eIDAS, podemos ver que, pese a tener implícitamente presente a lo largo de su articulado que la criptografía de clave asimétrica pública del emisor sigue predominando el funcionamiento actual de la firma electrónica, busca incidir más sobre el necesario principio de neutralidad tecnológica[556], eliminando toda referencia a la clave, en este caso privada, que, junto con su correspondiente clave pública, caracteriza el esquema

[555] RUBIO VELÁZQUEZ, R./MUÑOZ MUÑOZ, R./RODRÍGUEZ SAU, C., *La firma electrónica: aspectos legales y técnicos*, Barcelona, Experiencia, 2004, p. 133. Caso de emplear el sistema de cifrado criptográfico, los datos de creación de firma electrónica serían las claves privadas que sirven para descifrar (en el supuesto de cifrado de clave asimétrica pública del receptor) o para cifrar (en el supuesto de cifrado de clave asimétrica pública del emisor o firma digital) el documento electrónico (contrato por vía electrónica, en el supuesto que nos ocupa).

[556] ALMONACID LAMELAS, V. Y OTROS, «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», cit., p. 434. A favor de un planteamiento similar, *vid.* ELÍAS BATURONES, J. J., *La prueba de documentos electrónicos en los tribunales de justicia*, cit., p. 17; FERNÁNDEZ DOMINGO, J. I., *Algunas notas acerca de la contratación y el comercio electrónico*, cit., pp. 245; ILLESCAS ORTIZ, R., «La firma electrónica y el Real Decreto-ley 14/1999 de 17 de septiembre», cit., p. 7; ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., p. 15; MARTÍNEZ NADAL, A., «Comentarios de urgencia al urgentemente aprobado Real Decreto-ley 14/1999 de 17 de septiembre, sobre firma electrónica», cit., p. 1863; MORENO DELGADO, M. Y OTROS, «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», cit., pp. 201 a 203; RICO CARRILLO, M., «El Reglamento europeo sobre identificación y servicios de confianza electrónicos», cit., p. 20.

propio de la firma digital[557]. En cambio, en el texto anterior de la DFE –artículo 2.4)–, se incluía expresamente la referencia a estos «[…] códigos o claves criptográficas privadas», manteniendo, por lo demás, la misma redacción que el texto normativo actual; lo mismo sucederá en nuestro país con el artículo 2.d) RDLFE y, después, con el artículo 24.1 LFE, ambos idénticos, con la única salvedad, formal, de la diferente denominación empleada para designar al creador de la firma (signatario o firmante)[558].

Asimismo, el apartado 22) del artículo 3 RIE-SCTE entenderá por dispositivo de creación de firma electrónica el equipo o programa informático configurado que se utiliza para crear una firma electrónica[559]. Este dispositivo estará constituido por las aplicaciones de *software* y de *hardware* necesarias para generar la firma electrónica[560], permitiendo, para ello, la aplicación de los datos únicos de creación de firma electrónica por parte del autor o remitente para el cifrado del mensaje de datos a enviar[561]. Al igual que decíamos antes, la DFE marca, en cam-

[557] En concreto, el considerando 27 RIE-SCTE dispone que «[e]l presente Reglamento debe ser neutral en lo que se refiere a la tecnología. Los efectos jurídicos que otorga deben poder lograrse por cualquier medio técnico, siempre que se cumplan los requisitos que en él se estipulan».

[558] «[…] datos únicos, como códigos o claves criptográficas privadas, que el *signatario/firmante* utiliza para crear la firma electrónica» (la cursiva es propia, así como la fusión de ambas definiciones a efectos ilustrativos).

[559] A su vez, el apartado inmediatamente anterior –21)– define el término *producto* como el equipo o programa informático, o los componentes pertinentes del mismo, destinado a ser utilizado para la prestación de SSIisc. De ahí que, por ser la creación de firmas electrónicas un SSIisc, el dispositivo que sea utilizado por el PSSIisc para crear una firma electrónica responderá, al mismo tiempo, al concepto más general de *producto*. En cualquier caso, se trata esta de una definición confusa y ambigua –quién sabe si tanto como lo era la proporcionada por el artículo 2.12) DFE–, que no explicita qué diferencia puede haber entre estos productos y los dispositivos de creación y de verificación de firma electrónica; quizás se esté pensando en un producto comercial que ofrezca distintos servicios relacionados con la firma electrónica, como la generación de los datos de creación de firma electrónica u otros servicios complementarios.

[560] Por tanto, una cosa será el dispositivo de generación de los datos de creación de firma electrónica, que será aquel equipo o programa informático configurado que se utiliza para generar los datos de creación de firma electrónica, y otra el dispositivo de creación de firma electrónica propiamente dicho, que será, en cambio, aquel equipo o programa informático configurado que se utiliza para aplicar esos datos de creación de firma electrónica ya generados previamente por el dispositivo anterior.

[561] BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 427.

bio, un ligamen quizás más estrecho con los datos de creación de firma electrónica, definiendo estos dispositivos de creación como «[…] un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma» –artículo 2.5)–.

Este dispositivo tendrá un mayor plus de seguridad y, por tanto, adquirirá la condición de cualificado cuando cumpla los requisitos enumerados por el anexo II del Reglamento (antiguamente, apartado 6 del artículo 2 DFE[562]). Estos requisitos son los siguientes: en primer lugar, que el dispositivo cualificado de creación de firma electrónica garantice, como mínimo, por medios técnicos y de procedimiento adecuados, a) que esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas –antigua letra a), *in fine*, del apartado 1 del anexo III DFE–, b) que los datos de creación de firma electrónica utilizados para la creación de firma electrónica sólo puedan aparecer una vez en la práctica[563]–antigua letra a), *ab initio*, del apartado 1 del anexo III DFE–, c) que exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma electrónica está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento (principio de neutralidad tecnológica)[564] –antigua letra

[562] Que por dispositivo seguro (ahora, cualificado) de creación de firma electrónica entiende aquel «[…] dispositivo de creación de firma que cumple los requisitos enumerados en el anexo III».

[563] En la letra b) –también, sin duda, en la letra c), inciso primero– del apartado 1 del anexo II RIE-SCTE (de igual modo, en la normativa equivalente anterior) parece existir un error de concepto, ya que esta exigencia no hace referencia propiamente a los dispositivos de creación de firma electrónica, sino, más bien, a los dispositivos de generación de datos de creación de firma electrónica, de acuerdo a la distinción antes apuntada.

[564] En este caso, el legislador vuelve a referirse más a las características de los datos de creación de firma electrónica que a los dispositivos de creación de firma electrónica propiamente dichos (CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 148). En cualquier caso, ello permite sostener la interpretación de que esta exigencia establece simplemente una obligación de medios y no de resultado, de forma que es suficiente con establecer las medidas de protección, no exigiéndose el resultado de que las mismas eviten las acciones o actuaciones indicadas; una aproximación al carácter temporal de los certificados electrónicos puede verse en BLANCO URZÁIZ, J., «Sistema de tutela y gestión de los certificados digitales al amparo de la nueva Ley de firma electrónica», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 6, 2004, pp. 103 a 106. En cualquier caso, parece ser que, ya desde los tiempos de la DFE, la tecnología utilizada en el ámbito del cifrado (más concretamente los algoritmos matemáticos empleados) venía a garantizar de un modo razonable que no fuera posible deducir los datos de creación de firma electrónica

b) del apartado 1 del anexo III DFE– y d) que los datos de creación de firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su posible utilización por terceros[565] –antigua letra c) del apartado 1 del anexo III DFE–; en segundo lugar, que el dispositivo cualificado de creación de firma electrónica no altere los datos que deben firmarse ni impida que dichos datos se muestren al firmante antes de firmar, garantizando, de este modo, la integridad en el importante paso intermedio que existe entre la declaración de voluntad del firmante y la generación del documento firmado –antiguo apartado 2 del anexo III DFE–; en tercer lugar, que la generación o gestión de los datos de creación de firma electrónica en nombre del firmante sólo puedan correr a cargo de un PSSIisc –sin equivalente dentro del anexo III DFE–, y, en cuarto lugar, que, sin perjuicio de lo dispuesto en la letra d) anterior, los PSSIisc cualificados que gestionen los datos de creación de firma electrónica en nombre del firmante[566] puedan duplicar los datos de creación de firma electrónica únicamente con el objeto de efectuar una copia de seguridad de los citados datos, siempre que la seguridad de los conjuntos de datos duplicados sea del mismo nivel que para los conjuntos de datos originales y siempre que el número de

---

a partir de los datos de validación o verificación de la misma. Y es que, sobre la base de la capacidad con la que actualmente cuentan los ordenadores y teniendo en cuenta el tipo de algoritmos matemáticos y la longitud de las claves que normalmente suelen representar estos datos, sería poco probable llegar a conseguir la deducción, habida cuenta de que se tardaría un tiempo desproporcionado en conseguir averiguar los datos de creación de firma electrónica por medio de ataques basados en la "fuerza bruta" (*brute-force attacks*), entendiendo por tal la reiteración indeterminada de combinaciones posibles hasta encontrar la correcta (CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 51). Pese a ello, a nadie escapa que la seguridad en este punto es un concepto ciertamente relativo, ya que depende del estado de la tecnología existente en cada momento; de ahí que, a fin de evitar que en un futuro puedan deducirse los datos de creación de firma electrónica de documentos firmados en el presente, existen SSIisc como el *archiving*, regulado por primera vez, cuando es cualificado, en el artículo 34 RIE-SCTE; en ellos, un tercero independiente (el PSSIisc de conservación) almacena el documento (en este caso, el contrato) electrónico firmado, protegiéndolo con su propia firma electrónica, que se incorpora sucesivamente a dicho documento a medida que se van actualizando los dispositivos de creación de firma electrónica utilizados por el PSSIisc (RUBIO VELÁZQUEZ, R. Y OTROS, *La firma electrónica: aspectos legales y técnicos*, cit., p. 134).

[565] Como bien indica CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 151, no parece tener sentido condicionar que la firma electrónica sea cualificada al hecho de que los datos de creación de firma electrónica sean custodiados de una u otra manera.

[566] No se reconoce, por tanto, esta posibilidad a ninguna otra persona designada por el firmante.

conjuntos de datos duplicados no supere el mínimo necesario para garantizar la continuidad del servicio –sin equivalente dentro del anexo III DFE–.

Esta necesidad de satisfacer los requisitos del anexo II aparecerá reiterada en el artículo 29 Reglamento eIDAS. Además, en su apartado segundo, se otorga a la Comisión la posibilidad de que, por medio de actos de ejecución (que se adoptarán, en su caso, con arreglo al procedimiento de examen recogido en el artículo 48.2 RIE-SCTE), establezca números de referencia de normas relativas a los dispositivos cualificados de creación de firmas electrónicas; de ser así, se presumirá el cumplimiento de las condiciones introducidas en el anexo II cuando un dispositivo cualificado de creación de firmas electrónicas se ajuste a dichas normas. En cualquier caso, concluye el artículo 51.1 del Reglamento, los dispositivos seguros de creación de firma electrónica cuya conformidad se haya determinado con arreglo a lo dispuesto en el artículo 3.4 DFE tendrán la consideración de dispositivos cualificados de creación de firma electrónica con arreglo al RIE-SCTE.

En cualquier caso, el artículo 30 RIE-SCTE regula la certificación de los dispositivos cualificados de creación de firmas electrónicas por parte de los organismos públicos o privados adecuados designados por los Estados miembros[567], que notificarán sus nombres y direcciones a la Comisión, que, a su vez, deberá informar a los demás Estados miembros, pudiendo

[567] Este artículo se corresponde, sin cambios relevantes, con el artículo 3, apartados 4 y 5, DFE, que, sobre la base de cuanto dispone el considerando 15, establecía que «4. La conformidad de los dispositivos seguros de creación de firma con los requisitos fijados en el anexo III será determinada por los organismos públicos o privados pertinentes, designados por los Estados miembros. La Comisión, con arreglo al procedimiento del artículo 9, establecerá criterios para que los Estados miembros determinen si procede designar un determinado organismo. La conformidad con los requisitos del anexo III establecida por dichos organismos será reconocida por todos los Estados miembros. 5. La Comisión, con arreglo al procedimiento del artículo 9, podrá determinar, y publicar en el *Diario Oficial de las Comunidades Europeas*, los números de referencia de las normas que gocen de reconocimiento general para productos de firma electrónica. Los Estados miembros presumirán que los productos de firma electrónica que se ajusten a dichas normas son conformes con lo prescrito en la letra f) del anexo II y en el anexo III de la presente Directiva». Al amparo de la previsión contenida en el artículo 3.4 DFE surge la DCMO, sobre los criterios mínimos que deben tener en cuenta los Estados miembros para la designación de tales organismos. Por su parte, de la posibilidad atribuida a la Comisión al amparo del artículo 3.5 DFE nace la DPNRNPFE, sobre publicación de los números de referencia de las normas que gozan de reconocimiento general para productos de firma electrónica; tales normas, recogidas en el anexo de la Decisión, son las siguientes: A. Lista de normas que gozan de reconocimiento general para productos de firma electrónica considerados conformes por los Estados miembros con los requisitos del anexo II. f) de la Directiva 1999/93/CE: 1) CWA 14167-1 (marzo de 2003): *security requirements for trustworthy systems managing certificates for electronic signatures*

adoptar actos delegados (de conformidad con el artículo 47 del Reglamento) en relación con el establecimiento de criterios específicos que deban satisfacer los organismos designados[568]. Esta certificación permitirá determinar la conformidad de los dispositivos cualificados de creación de firmas electrónicas con los requisitos del anexo II[569], certificación que se basará en dos procesos diferentes: de un lado, un proceso de evaluación de la seguridad, llevado a cabo de acuerdo con las normas para la evaluación de la seguridad de los productos de tecnología de la información incluidos en la lista que, por medio de actos de ejecución (que se adoptarán con arreglo al procedimiento de examen contemplado en el artículo 48.2 RIE-SCTE), será establecida por la Comisión; de otro, un proceso distinto del anterior, que será válido a condición de que, en primer lugar, haga uso de niveles de seguridad equivalentes; en segundo lugar, los organismos públicos o privados designados lo notifiquen a la Comisión, y, en tercer lugar, no existan las normas para la evaluación de la seguridad de los productos de tecnología de la información antes citadas o cuando esté en curso el proceso de evaluación de la seguridad anterior[570]. De esta última exigencia, tan sólo podría darse la segunda de ellas

— Part 1: *System Security Requirements*; 2) CWA 14167-2 (marzo de 2002): *security requirements for trustworthy systems managing certificates for electronic signatures* — Part 2: *cryptographic module for CSP signing operations — Protection Profile* (MCSO-PP). B. Lista de normas que gozan de reconocimiento general para productos de firma electrónica considerados conformes por los Estados miembros con los requisitos del anexo III de la Directiva 1999/93/CE: CWA 14169 (marzo de 2002): *secure signature-creation devices*.

[568] Nada se indica en el Reglamento eIDAS, como tampoco en el ALSEC, respecto de los sujetos que podrán solicitar la certificación. No obstante, si atendemos a lo dispuesto en la LFE, a la que más adelante prestaremos atención, esta certificación de dispositivos cualificados de creación de firma electrónica podrá ser solicitada por el fabricante de dicho dispositivo o, en su caso, por su importador (artículo 27.2 LFE).

[569] Aplicado a nuestro país, el RIE-SCTE sigue la estela de la LFE, en la que disminuye significativamente la importancia de obtener el certificado de conformidad de los dispositivos seguros de creación de firma electrónica respecto del RDLFE; esta última norma otorgaba la presunción de que la firma electrónica avanzada reunía las condiciones necesarias para producir los efectos indicados en el artículo 3 cuando contaba con un dispositivo seguro certificado y con un certificado electrónico reconocido expedido por un PSSIic acreditado (artículo 3.1.2º RDLFE). En cualquier caso, se mantiene su importancia desde un punto de vista comercial, toda vez que el dispositivo certificado aparecerá en el mercado como un dispositivo que ofrece una mayor fiabilidad y seguridad frente a aquellos que no lo están, en la medida en que se ha visto sometido a un procedimiento voluntario de control por parte de entidades independientes que ha culminado con la concesión de dicha certificación.

[570] Como ya sucediera con los artículos 3.4 DFE y 27 LFE, no queda claro si es necesario, a fin de que el dispositivo de creación de firma electrónica sea cualificado, obtener una certificación *a priori* por el/los organismo/s encargado/s de determinar la conformidad de tales dispositivos con los requisitos que figuran en el

(que esté en curso un proceso de evaluación de la seguridad), ya que, con fecha de 26 de abril de 2016, tuvo lugar la publicación en el DOUE de la DENESDCCFS.

Una vez certificados conforme a lo dispuesto en el párrafo anterior, los Estados miembros deberán comunicar a la Comisión (con los formatos y procedimientos definidos, en su caso, por la misma a través de actos de ejecución adoptados con arreglo al artículo 48.2) información de los dispositivos cualificados de creación de firmas electrónicas afectados, sin retrasos indebidos y, a más tardar, en el plazo de un mes desde que haya concluido la certificación. La misma información tendrán que proporcionar respecto de aquellos dispositivos cualificados de creación de firmas electrónicas cuya certificación haya expirado, siendo también de un mes el plazo para hacerlo, si bien en este caso a contar desde que se haya producido la expiración. Todo ello permitirá a la Comisión establecer, publicar y mantener una lista de dispositivos cualificados de creación de firmas electrónicas con certificación actualizada (artículo 31 RIE-SCTE).

En España, el artículo 2.e) RDLFE dio paso al artículo 24.2 LFE[571], que, con una misma redacción, definió el dispositivo de creación de firma electrónica con una redacción que hacía más hincapié que la actual en su relación con los datos de creación de firma electrónica: «[…] programa o sistema informático *que sirve para aplicar los datos de creación de firma*»[572]. A su vez, el artículo 24.3 LFE –previamente, artículos 2.f) y 19 RDLFE– establecía también los requisitos que debía cumplir el dispositivo de creación de firma electrónica que quisiera tener el calificativo de seguro: a) que los datos utilizados para la generación de la firma electrónica pudieran producirse sólo una vez y asegurasen razonablemente su secreto[573] –letras a) y b) del

anexo II. Y es que también cabría la posibilidad de cumplir esta disposición si la certificación de los dispositivos de creación de firma electrónica es, simplemente, un distintivo voluntario de calidad; de este modo, planteado un conflicto al respecto, el tribunal o las propias partes podrían encargar a este organismo designado por el Estado miembro la verificación *a posteriori* de los requisitos para que el dispositivo fuera seguro. Tampoco quedan claros los efectos que conllevaría esta declaración de conformidad, en tanto no especifica si el juez estará vinculado por la misma a la hora de determinar el cumplimiento de los requisitos o si tan sólo se trata de algún tipo de presunción al respecto.

[571] En países como Italia, al actual artículo 35 CAD, que mencionan algunos de los requisitos a cumplir por estos dispositivos y se remiten, al mismo tiempo, a cuantos se contienen en el anexo II RIE-SCTE.

[572] La cursiva es propia.

[573] Como apuntábamos al hablar del RIE-SCTE, pese al tenor literal de esta letra a), en ningún caso los dispositivos de creación de firma electrónica podrán garantizar que la clave de cifrado empleada pueda producirse

apartado 1 del anexo II RIE-SCTE y antiguo artículo 19.1º RDLFE–; b) que existiese una seguridad razonable de que los datos de creación de firma electrónica no pudiesen ser derivados de los datos de verificación de la misma o de la propia firma electrónica y de que esta se hallase protegida contra la falsificación por medio de la tecnología existente en cada momento –letra c) del apartado 1 del anexo II RIE-SCTE y antiguo artículo 19.2º RDLFE–; c) que los datos de creación de firma electrónica pudiesen ser protegidos de forma fiable por el firmante contra su utilización por terceros –letra d) del apartado 1 del anexo II RIE-SCTE y antiguo artículo 19.3º RDLFE–, y d) que el dispositivo de creación de firma electrónica utilizado no alterase los datos o el documento que debiera firmarse ni impidiese que este se mostrase al firmante antes del proceso de firma electrónica –apartado 2 del anexo II RIE-SCTE y antiguo artículo 19.4º RDLFE–. Se presumía que los productos de firma electrónica del artículo 24.3 LFE eran conformes con los requisitos previstos en dicho artículo si se ajustaban a las normas técnicas correspondientes, cuyos números de referencia hubiesen sido publicados en el DOUE (artículo 28.1 LFE, sobre la base del artículo 3.5 DFE).

Además, siguiendo la previsión de los apartados 4 y 5 del artículo 3 DFE se crean los artículos 27 y 28.2 LFE (antes, artículos 20 y 21 RDLFE). El primero de ellos, tras definir la certificación de dispositivos seguros de creación de firmas electrónicas en los términos de conformidad a la normativa ya apuntados, sostiene que esta podrá ser solicitada por los fabricantes o importadores de este tipo de dispositivos, siendo llevada a cabo (utilizando las normas técnicas cuyos números de referencia hayan sido publicados en el DOUE y, excepcionalmente, las aprobadas por el ahora Ministerio de Energía, Turismo y Agenda Digital[574], a publicar en su correspondiente dirección de Internet –no requiriendo, por tanto, de publicación oficial–) por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la LI y en sus normas de desarrollo. Asimismo,

una sola vez; esta cuestión sólo puede ser garantizada por los dispositivos de generación de los datos de creación de firma electrónica. Sin embargo, para hacer aplicable esta garantía, sería posible realizar una interpretación en el sentido de considerar que el dispositivo de creación de firma electrónica debe utilizar unos datos de creación de firma electrónica seguros. Esta interpretación presenta, no obstante, el inconveniente de que poco tiene que ver con el dispositivo de creación de firma electrónica como tal. Resultado de lo anterior, podemos entender inadecuada la ubicación de esta previsión en el texto de la norma.

[574] El Ministerio de Ciencia y Tecnología fue derogado por la D. F. 1ª ARDRDM (BOE núm. 94, de 18 de abril de 2004). En la actualidad, las tareas de este órgano son asumidas por el Ministerio de Energía, Turismo y Agenda Digital, merced al artículo 10 RDRDM.

añade, estos certificados serán modificados o, en su caso, revocados cuando se dejen de satisfacer las condiciones que permiten su obtención, habiendo de ser difundida la decisión de revocación por los organismos de certificación designados. El segundo precepto, por su parte (sobre la base del artículo 3.4.2º DFE), afirma expresamente en su apartado segundo que «[s]e reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo» (interoperabilidad de los dispositivos de firma electrónica certificados entre los distintos Estados miembros, no prevista explícitamente en los artículos 30 y 31 RIE-SCTE ni en el ALSEC).

### 3.2. Datos y dispositivos de verificación o validación

La parte complementaria de los datos de creación de firma electrónica son los datos de verificación o validación de la misma, definidos en la actualidad en el artículo 3.40) RIE-SCTE como «[…] los datos utilizados para validar una firma electrónica», entendiéndose por validación a estos efectos el proceso de verificar y confirmar la validez de una firma electrónica –artículo 3.41) RIE-SCTE–[575]. Al igual que hicimos constar en el apartado correspondiente a los datos de creación de firma electrónica, conviene subrayar la ausencia de cualquier alusión específica por parte del Reglamento eIDAS a las claves públicas, necesarias (en su conjunción con las claves privadas) para conformar la firma digital, mecanismo criptográfico todavía imperante a la hora de garantizar la identificación autenticada, la autenticación, la integridad y el no repudio de los mensajes de datos necesarios para la celebración de un contrato por vía electrónica. Y ello, recordemos, en un intento por reforzar el principio de neutralidad tecnológica que, aun existente también en la normativa anterior, resultaba algo más difuso que ahora; en efecto, los artículos 2.g) RDLFE, 2.7) DFE y 25.1 LFE coinciden en definir los datos de verificación de firma electrónica como aquellos «[…] datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica» (definición proporcionada por este último precepto).

[575] Siguiendo, por relevante, con el ejemplo del sistema de cifrado criptográfico, los datos de verificación o validación vendrán representados por las claves públicas que permitirán la operación inversa a las claves privadas: cifrar (en el caso de optar por el supuesto de cifrado de clave asimétrica pública del receptor) o descifrar (en el supuesto de elegir el cifrado de clave asimétrica pública del emisor o firma digital) el documento (contrato) electrónico.

Sin embargo, sin motivo aparente alguno, el RIE-SCTE opta por suprimir toda referencia a los dispositivos de verificación o validación de firma electrónica (no así, como hemos podido ver, con los dispositivos de creación, que permanecen). En ello, la norma se diferencia de manera sustancial de su predecesora, que, entre su articulado, incorporó un artículo 2.8) en el que definía los dispositivos de verificación de firma electrónica como aquellos programas o aparatos informáticos configurados que sirven para aplicar los datos de validación de firma electrónica. Estos dispositivos vendrían constituidos por aquellas otras aplicaciones de *software* y de *hardware* que sirven para verificar la firma electrónica, haciendo necesaria, como paso previo, la aplicación de los datos de verificación de firma electrónica por parte del destinatario para el descifrado del mensaje de datos a recibir. En la misma línea se encontrará también el artículo 25.2 LFE que, al igual que el artículo 2.h) RDLFE, se hallan presididos en este punto por una fuerte influencia comunitaria.

En cualquier caso, ha de ponerse de manifiesto que el dispositivo de creación de firma electrónica empleado por el firmante y el dispositivo de verificación o validación de firma electrónica utilizado por el receptor del mensaje de datos no constituyen, a diferencia de lo que sucedía con la clave privada y con la clave pública, un par único y relacionado, de suerte que puede darse el caso de que uno y otro tengan distintos niveles de calidad y de seguridad. Tanto es así que, aun cuando tradicionalmente se han establecido una serie de requisitos que deberían garantizar los dispositivos de verificación, no se ha contemplado legalmente un procedimiento de certificación de la seguridad de los mismos[576].

En cualquier caso, sí que establece el Reglamento las exigencias que habrá de satisfacer todo proceso que quiera confirmar la validez de una firma electrónica cualificada, no pronunciándose respecto del resto de modalidades de firma. Estas exigencias quedan concretadas en las siguientes (artículo 32.1 RIE-SCTE): a) que el certificado electrónico que respalda la firma electrónica fuera, en el momento de la firma, un certificado cualificado de firma electrónica sujeto al anexo I –sin equivalente dentro del anexo IV DFE–; b) que el certificado electrónico cualificado fuera emitido por un PSSIisc (entiendo que cualificado) y fuera válido en el momento de la firma –en parte, antigua letra d) del anexo IV DFE–; c) que los datos de validación de la firma electrónica correspondan a los datos proporcionados a la parte

[576] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 476.

usuaria[577] –antigua letra a) del anexo IV DFE–; d) que el conjunto único de datos que representa al firmante en el certificado electrónico se facilite correctamente a la parte usuaria –sin equivalente dentro del anexo IV DFE–; e) que, en caso de que se utilice un seudónimo, la utilización del mismo se indique claramente a la parte usuaria en el momento de la firma –antigua letra f) del anexo IV DFE–; f) que la firma electrónica se haya creado por medio de un dispositivo cualificado de creación de firma electrónica –sin equivalente dentro del anexo IV DFE–; g) que la integridad de los datos firmados electrónicamente no se haya visto comprometida –sin equivalente dentro del anexo IV DFE–, y h) que se hayan cumplido los requisitos previstos en el artículo 26 RIE-SCTE (requisitos de la firma electrónica avanzada) en el momento de la firma –sin equivalente dentro del anexo IV DFE–. Además, el sistema empleado para validar la firma electrónica cualificada ofrecerá a la parte usuaria el resultado correcto del proceso de validación –antigua letra b) del anexo IV DFE– y le permitirá, además, detectar cualquier problema que afecte a la seguridad –antigua letra g) del anexo IV DFE– (artículo 32.2 RIE-SCTE). Por último, se faculta a la Comisión para, mediante actos de ejecución (a adoptar, en su caso, con arreglo al procedimiento de examen contemplado en el artículo 48.2 Reglamento eIDAS), establecer números de referencia de normas relativas a la validación de firmas electrónicas cualificadas, presumiéndose el cumplimiento de los requisitos establecidos en el artículo 32.1 cuando la validación de una firma electrónica cualificada se ajuste a dichas normas (artículo 32.3 RIE-SCTE).

Tanto más, incorpora un artículo 33 (sin precedentes de ningún tipo, ni comunitarios ni nacionales) que establece los requerimientos que deberán satisfacer los PSSIisc cualificados que quieran prestar un SSIisc de validación cualificado de firmas electrónicas cualificadas. En concreto, se reducen a dos: en primer lugar, que dicho PSSIisc cualificado realice la validación cumpliendo lo dispuesto en el artículo 32.1 anterior; en segundo lugar (y es aquí donde, entiendo, radica la nota diferencial que permite calificar el SSIisc como cualificado), que este mismo PSSIisc cualificado permita que las partes usuarias reciban el resultado del proceso de validación (artículo 32.2, *ab initio*) de una manera automatizada que sea fiable, eficiente e incluya la firma electrónica avanzada o el sello electrónico avanzado del PSSIisc de validación cualificado. Sin embargo, no añade, al menos aparentemente, que el sistema utilizado para validar la firma electrónica cualificada permita detectar cualquier problema que afecte a la

[577] Con este término se aludirá a la persona física o jurídica que confía en la identificación electrónica o el servicio de confianza –artículo 3.6) RIE-SCTE–.

seguridad, como sí hace el inciso final del artículo 32.2. También aquí se otorga a la Comisión la facultad de establecer, mediante actos de ejecución a adoptar con arreglo al procedimiento del artículo 48.2 RIE-SCTE, números de referencia relativos al SSIisc de validación cualificado, de tal suerte que, de ajustarse la firma electrónica cualificada a dichas normas, se presumirá el cumplimiento de los requisitos establecidos en el artículo 33.1.

En España, el artículo 25.3 LFE (artículo 22 RDLFE) establece los requisitos para la validación de la firma electrónica general, a diferencia del RIE-SCTE, que sólo se refiere a la firma electrónica cualificada. En concreto, resuelve este precepto que los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación satisfaga, como mínimo, una serie de condiciones (que, aunque no lo diga expresamente, harían que el dispositivo tuviera la consideración –en coherencia con el resto de la norma– de dispositivo seguro de verificación de firma electrónica): a) que los datos utilizados para verificar la firma electrónica correspondan a los datos mostrados a la persona que verifica la misma –letra c) del artículo 32.1 RIE-SCTE, sin equivalente en el RDLFE–; b) que la firma electrónica se verifique de forma fiable y el resultado de esa verificación se presente correctamente –en parte, artículo 32.2 RIE-SCTE y antiguo artículo 22.1.1 RDLFE–; c) que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados –sin equivalente en el artículo 32.1 RIE-SCTE y antiguo artículo 22.1.2 RDLFE–; d) que se muestren correctamente tanto la identidad del firmante (o, en su caso, conste claramente la utilización de un seudónimo) como el resultado de la verificación –en parte, letra e) del artículo 32.1 RIE-SCTE y antiguo artículo 22.1.3 RDLFE–; e) que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente –en parte, letra b) del artículo 32.1 RIE-SCTE y antiguo artículo 22.1.4 RDLFE–, y f) que pueda detectarse cualquier cambio relativo a su seguridad –en parte, artículo 32.2 RIE-SCTE y antiguo artículo 22.1.5 RDLFE–. Sin embargo, a diferencia de lo que sucedía respecto de los dispositivos seguros de creación de firma electrónica, la LFE no contempla la posibilidad de que los dispositivos "seguros" de verificación de la misma sean certificados[578]. Por último, añade el

[578] En este sentido, *Ibid.*, p. 479, destacaba la conveniencia jurídica y comercial de conceder esta posibilidad de certificación, que permitiría «[…] dar seguridad al funcionamiento de la firma electrónica y los productos asociados con la misma; resultando positiva tanto para los usuarios de tales productos, especialmente si son consumidores, como para los propios empresarios que crean o comercializan tales productos, en la medida que les

artículo 25.4 LFE, «[…] los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento[579], podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza»[580] –sin equivalente en el artículo 32 RIE-SCTE ni en el artículo 22 RDLFE–.

4. Concepto y clases de firma electrónica

Ya dijimos al hablar de los elementos esenciales de todo documento que, como regla general y en virtud del principio de libertad de forma que impera en nuestro ordenamiento jurídico, la firma, en cuanto componente accesorio, no afecta a la validez y eficacia de los contratos, que podrán existir con independencia de aquella e, incluso, del soporte físico que les confiere corporeidad. No obstante, motivos de seguridad aconsejan su utilización como medio de atribución del mensaje de datos a un sujeto concreto, así como para la determinación de los efectos jurídicos que dicho mensaje pueda llegar a desplegar; de lo contrario, tendremos que acudir a medios de prueba complementarios e indirectos, no siempre disponibles pero, con frecuencia, ineficaces y del todo complejos. Lo mismo sucede en el ámbito del *e-commerce*, donde la firma electrónica, en principio, no es preceptiva y los contratos que de ella carecen pueden ser totalmente válidos, siendo recomendable, empero, su empleo

permiten aparecer en el mercado con un plus de seguridad, con una garantía superior a la de los productos no certificados».

[579] Llama la atención que la LFE se refiera a la constancia del momento en el que se verifica la firma electrónica, ya que lo relevante, en realidad, ha de ser el momento en el que esta es creada, a fin de determinar si el certificado electrónico estaba o no vigente en ese momento.

[580] Este tercero de confianza podría venir personificado por el PSSIisc o por un notario, siendo esta segunda opción, en opinión de BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 436, posiblemente más adecuada, ya que, en caso de disputa entre el firmante y el verificador (único de los dos autorizado –no entendemos el motivo– por el artículo 25.4 LFE para el almacenamiento de los datos referentes a la verificación de la firma electrónica), este tercero tendrá, presumiblemente, una actuación más independiente y objetiva, ofreciendo mayores garantías para unas partes que, entonces sí, podrían estar actuando en condiciones de igualdad.

como vía de aseguramiento de la identidad de los intervinientes y de la integridad de sus declaraciones[581].

A continuación, analizamos la firma electrónica desde una perspectiva legal (más concretamente, las firmas electrónicas, un total de tres, determinantes de cada una de las tres clases recogidas por la normativa nacional y comunitaria). Para ello, acudiremos al Reglamento europeo en materia de identificación electrónica y servicios de confianza para las transacciones electrónicas (artículos 3 y 25 a 34), en un estudio que se verá acompañado en determinados aspectos por cuanto expone la LFE (y, en menor medida, el primigenio RDLFE), norma esta última que, por reflejar la incorporación a España de la ya derogada DFE, resulta interesante a efectos comparativos y, hasta el momento en que se produzca su derogación –quien sabe si por el texto del ALSEC, del que también nos hacemos eco–, complementarios[582].

### 4.1. Firma electrónica general *versus* firma electrónica simple

El artículo 3.10) RIE-SCTE define de forma general la firma electrónica como «[…] los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar»[583], o, lo que es lo mismo, cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención

[581] En todo caso, como bien hiciera constar VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., pp. 143 y 144, remitiéndose, a su vez, a DE ROSELLÓ MORENO, R., *El comercio electrónico y la protección de los consumidores*, cit., p. 43, conviene precisar que «[…] desde un punto de vista semántico habría que hacer la precisión de que la firma electrónica no se apoya en la idea de ser, en cuanto a la confección de puño y letra, del autor, aunque sirve para reflejar la autoría de un documento, por lo que al menos la Ley se esfuerza en dotarle de ese reconocimiento otorgando a la firma electrónica análogo valor que a la firma tradicional»; en la misma línea, MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., p. 131.

[582] Como indica el ALSEC en el punto primero de su Exposición de Motivos, desde el 1 de julio de 2016 resulta de aplicación el RIE-SCTE, de modo que la LFE se encuentra, desde entonces, «[…] jurídicamente desplazada por el citado Reglamento en todo aquello no regulado por él».

[583] Así, el RIE-SCTE, siguiendo la tradición normativa anterior, conserva el nombre de *firma electrónica* para referirse a aquella firma electrónica distinta de la firma electrónica avanzada y a la firma electrónica cualificada; sobre esta cuestión, *vid.* VATTIER FUENZALIDA, C., «El régimen legal de la firma electrónica», cit., pp. 413 y 414.

de firmar, cumpliendo todas o algunas de las funciones características de la firma autógrafa[584]. La referencia a su utilización con la intención de firmar se corresponde con la nueva regulación de otros servicios electrónicos de confianza que responden a fines diferentes[585].

Esta definición pone de manifiesto la intención del legislador comunitario de regular las firmas electrónicas en sentido amplio, sin perjuicio de disciplinar con más detalle modalidades específicas a las que, de manera gradual, atribuye una especial eficacia jurídica –por orden ascendente, firmas electrónicas avanzadas y firmas electrónicas cualificadas–. Asimismo, se trata de un concepto tecnológicamente indefinido[586] (principio de neutralidad tecnológica), ya que no se refiere a ninguna tecnología específica (criptografía, *passwords*, etc.) a través de la cual se deba firmar, si bien es cierto que será la criptografía asimétrica propia de la firma digital, la que, de manera velada, presida el conjunto de la norma. Por lo demás, los datos que integran la firma electrónica podrán formar parte del documento electrónico o ir asociados formalmente con ellos, apareciendo como un conjunto independiente; este modo, integrado o separado, en que, en su caso, se manifieste la firma electrónica dependerá del sistema técnico seleccionado y de las aplicaciones prácticas con que cuente cada modalidad.

---

[584] Con carácter previo a esta distinción entre modalidades de firma electrónica, RAIMONDO, F., «Firme "digitali", crittographia e validità del documento elettronico», *Il diritto dell'informazione e dell'informatica*, vol. 1, 1996, p. 155, define la firma electrónica en abstracto como «[…] un conjunto de caracteres alfanuméricos resultante de complejas operaciones matemáticas de criptografía efectuadas por un ordenador sobre un documento electrónico», eliminando, por completo, el, pretendido por la norma, principio neutralidad tecnológica. En la misma línea, FORCADA MIRANDA, F. J., «El registro de la propiedad y las nuevas tecnologías: la publicidad formal, acceso al proceso y efectos jurídicos», *Estudios de Derecho judicial*, vol. 43, 2002, pp. 107 y 108, quien la define como «[…] un resumen cifrado de un mensaje», de modo que firmar un documento «[…] supone cifrarlo para convertirlo en otro distinto e ilegible pero relacionado con el documento original gracias al algoritmo de cifrado»; MADRID PARRA, A., «Aspectos jurídicos de la identificación en el comercio electrónico», cit., p. 193, al entenderla como el proceso, generalmente digital, en el que, por medio de la realización de un cálculo matemático sobre la base de un algoritmo, se lleva a cabo el cifrado de un concreto mensaje electrónico, de forma que sólo es posible el descifrado, es decir, el acceso al mensaje original, mediante la aplicación del correspondiente algoritmo o clave para realizar el proceso de naturaleza inversa; RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., p. 45, al aportar una definición de firma electrónica como el mensaje electrónico «[…] cuando ha sido ya codificado mediante el dispositivo de creación de firma».

[585] DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 132.

[586] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 74.

De acuerdo con esta noción general, firma electrónica podría ser, en términos contractuales, cualquier conjunto de datos basado en medios electrónicos y utilizado por el contratante firmante con la intención de firmar, sin especificar (en un intento, entiendo, por dejar abierta la firma electrónica a cuantas finalidades le permitan los sucesivos avances tecnológicos) el fin perseguido al hacerlo. Se incurre, de este modo, en una especie de redundancia un tanto incomprensible, que lleva a definir la firma electrónica general como aquella que utiliza el firmante para firmar.

En este punto, el Reglamento eIDAS se separa de la definición recogida por su precedente, la DFE –artículo 2.1)–, que, proporcionando un concepto de firma electrónica simple[587] (no general), circunscribía el fin común perseguido por toda firma electrónica a servir como medio de autenticación[588]. Y ello en una redacción, a mi juicio, discutible[589] y generadora de confusión, ya que, por ser esta fase de autentificación posterior a la de identificación propiamente dicha, hubiera sido mejor optar por esta última[590]; así lo hace, precisamente, el

---

[587] VALERO TORRIJOS, J./MARTÍNEZ GUTIÉRREZ, R., «Las bases jurídicas de la modernización tecnológica en las Administraciones públicas», en PLAZA PENADÉS, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, p. 531; VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., p. 158.

[588] De acuerdo con este precepto, por firma electrónica se entenderán aquellos «[…] datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación». El origen del empleo de este término por la DFE se remite directamente al concepto anglosajón *authentication*, concebido como la esencia del acto de la firma, el acto de suscripción del documento (CRUZ RIVERO, D., «Las definiciones de firma electrónica en el Real Decreto-ley 14/1999, sobre firma electrónica, y el Proyecto de Ley de firma electrónica», en DAVARA RODRÍGUEZ, M. Á. (coord.) *XVIII Encuentros sobre Informática y Derecho, 2003-2004*, Madrid, Universidad Pontificia de Comillas, 2004, pp. 127 a 136).

[589] No lo entiende así, en cambio, CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 41, quien sostiene que, a diferencia de la *identificación*, el empleo del término *autenticación* denota una actuación consciente de suscribir una declaración. Por su parte, ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 723, concluye, en una interpretación amplia de ambos preceptos (comunitario y nacional), que, con carácter general, la DFE y la LFE «[…] permiten el empleo, como sistema de firma electrónica, de cualesquiera mecanismos de identificación/autenticación, siempre que los mismos resulten apropiados para el contexto de la operación de que se trate, y que sólo se podrían considerar excluidos de la definición legal aquellos sistemas técnicamente diseñados para ser anónimos».

[590] El artículo 3.1) RIE-SCTE define la identificación electrónica como el proceso de utilizar los datos de identificación de una persona [es decir, el conjunto de datos que permite establecer la identidad de una persona

legislador español[591], tanto en el originario artículo 2.a) RDLFE[592] como en el artículo 3.1 LFE[593], preceptos ambos que hablan de la firma simple como medio que permite, en todo

---

física o jurídica, o de una persona física que representa a una persona jurídica –artículo 3.3)–] en formato electrónico, siendo estos los datos que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

[591] En opinión de CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 16, «[…] la única razón por la que el legislador español huye de esta expresión como elemento definidor de la firma electrónica es el deseo de dejar claro que el acto de la firma es propio del emisor del mensaje, suscriptor del documento, sin que sea necesaria la intervención notarial, a la vez que se quiere erradicar toda duda respecto a la naturaleza de los prestadores de servicios de certificación».

[592] Que define la firma electrónica como «[…] conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge»; sobre esta definición, *vid.* ALCOVER GARAU, G./ALONSO UREBA, A., «La firma electrónica», en DE ROS CEREZO, R. M./CENDOYA MÉNDEZ DE VIGO, J. M. (coords.) *Derecho de Internet : la contratación electrónica y firma digital*, Cizur Menor, Aranzadi, 2000, p. 192, niegan que el adjetivo *formal* implique una graduación en la identificación.

[593] «[…] La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante». La definición contenida en el artículo 3.1 LFE es exactamente la misma que la recogida en el Proyecto de Ley que se presentó a las Cortes para su posterior tramitación parlamentaria; no sucede así, en cambio, con las dos versiones que la precedieron: la versión primera, de principios de 2002, definía esta firma electrónica como «[…] conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar al autor o a los autores del documento que la recoge», en línea con el RDLFE; la versión segunda, de 26 de julio de ese mismo año, la conceptualizaba como «[…] conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio de autenticación», en una redacción más próxima a la DFE. Por lo demás, conviene detenerse en la, en mi opinión, inadecuada estructura que presenta el medular artículo 3 LFE tras la tramitación parlamentaria experimentada por el Proyecto de Ley. Este artículo, que tiene por título *firma electrónica, y documentos firmados electrónicamente* (también inadecuado, pues, al no adaptarse a la modificación experimentada en la noción del apartado quinto por parte de la LMISI, parece dejar al margen a aquellos documentos electrónicos en que no conste firma electrónica), lejos de regular ambos aspectos de manera ordenada, intercala apartados concernientes indistintamente a uno u otro, o a ambos, generando una confusión que se hubiera podido evitar sin excesiva complejidad; así, una propuesta de reformulación del precepto conforme al siguiente orden permitiría entender más fácilmente cuanto en él se contiene: 1) definición inicial de firma electrónica simple; 2) sobre la base de la anterior, definición de firma electrónica avanzada; 3) sobre la base de la anterior, definición de firma electrónica reconocida; 4) una vez definidos los tres tipos de firma electrónica contemplados por la Ley, regulación de los efectos

caso, *identificar a quien firma* en relación con unos datos[594] (en términos análogos al rol que cumple la firma manuscrita[595])[596], con independencia de que, posteriormente, se compruebe que la persona física que plasma su rúbrica[597] sobre el documento electrónico es quien dice

jurídicos generales de toda firma electrónica; 5) especificación de los efectos jurídicos propios de la firma electrónica reconocida, por ser la dotada de un mayor nivel de seguridad; 6) concreción de los efectos jurídicos de los sistemas de identificación y firma electrónica en el ámbito del sector público; 7) determinación de los efectos jurídicos de aquellas firmas electrónicas que, no recogidas por la Ley, sean utilizadas por las partes; 8) una vez regulada la firma electrónica, delimitación legal del documento electrónico, comenzando por la definición; 9) tras la definición, su posible naturaleza, pública o privada; 10) para concluir, su valor y eficacia; 11) una vez regulados por separado la firma electrónica y el documento electrónico, análisis conjunto del valor probatorio de los documentos firmados electrónicamente. Por lo demás, para un estudio más profundo de este precepto, *vid.* PAREJO NAVAS, T., «Análisis de las figuras esenciales del régimen jurídico de la firma electrónica la ley 59/2003, de 19 de diciembre de firma electrónica», *Revista de la contratación electrónica*, vol. 70, 2006, pp. 3 a 32.

[594] Por tanto, todo dato recogido en forma electrónica que cumpla una función identificativa, con independencia del nivel de seguridad que ofrezca, puede ser considerado como firma electrónica (MADRID PARRA, A., «La identificación en el comercio electrónico», *Revista de la contratación electrónica*, vol. 15, 2001, p. 17).

[595] El artículo 7 LMCE, a la hora de regular con carácter general el equivalente funcional de la firma, estableciendo los requisitos de admisibilidad de una firma producida por medios electrónicos, establece que las funciones tradicionales de una firma manuscrita son: a) identificar a una persona, b) proporcionar certidumbre en cuanto a su participación personal en el acto de una firma y c) vincular a esa persona con el contenido del documento. No se exige que la firma manuscrita proporcione integridad al documento, posible, con matices, en el caso de documentos manuscritos, imposible en el caso de documentos mecanografiados o impresos (MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 74).

[596] También a nivel internacional por el, aún más amplio y explícito, artículo 2.a) LMFE, que por firma electrónica entiende «[…] los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos». Igualmente, en Italia, el actual artículo 1.q) CAD, que define este tipo básico de firma electrónica como «[…] l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica», es decir, «[…] el conjunto de datos en forma electrónica, adjuntados o conectados mediante asociación lógica a otros datos electrónicos, utilizados como método de identificación informática»; sobre este precepto, *vid.* DI COCCO, C. Y OTROS, *Temi di Diritto dell'informatica*, cit., p. 52.

[597] A lo largo de este estudio, identificaremos *firma* y *rúbrica* como términos sinónimos o equivalentes. A favor de esta equiparación, CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 20, que sostiene que «[e]l carácter manuscrito de la firma constituye, precisamente por su capacidad probatoria, un rasgo constitutivo de la institución, de modo que suelen asimilarse legalmente la firma, que indica la identidad del firmante, y la rúbrica, de carácter ilegible».

ser[598]. Pese a lo anterior, bien es cierto, ni una ni otra aclaran qué ha de entenderse por autenticación y por identificación, lo que nos sitúa ante un concepto jurídico indeterminado susceptible de generar interpretaciones radicalmente distintas[599].

Como quiera que sea, lo cierto es que, con esta nueva redacción, la norma europea genera una confusión en nada desdeñable. En efecto, si con la DFE quedaba delimitado (aun con objeciones, como hemos dejado patente) el *mínimo* que debía cumplir toda firma electrónica para ser considerada como tal a efectos jurídicos (identificación del firmante de un mensaje de datos o autenticación o acreditación de dicha identificación[600]), el RIE-SCTE, pese a la plausible intención presumiblemente perseguida, imposibilita al jurista la concreción del elemento que, satisfecho, permita saber cuándo nos hallamos en presencia de una firma electrónica, por básica o elemental que sea; en consecuencia, dentro de esta definición, tendrían cabida procedimientos múltiples de firma, algunos tan complejos como la firma digital basada en la criptografía asimétrica o la firma configurada sobre la base de sistemas biométricos como el iris, la palma de la mano o la huella dactilar[601] y otros tan simples como la plasmación

[598] Como críticas al carácter excesivamente neutro de los preceptos de la DFE y de la LFE en este punto, *vid.* DELFINI, F., *Contratto telematico e commercio elettronico*, Milán, Giuffrè, 2002, p. 65 y VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., pp. 143 y 144. Según este último autor, «[…] lo que se pretende expresar es que con la firma electrónica se declara la autoría de un determinado documento electrónico y se permite a los terceros tener la certidumbre de que dicho documento les llega íntegro e inalterado y que la ley imputa al sujeto signante las consecuencias jurídicas derivadas del mismo, con lo cual se quiere evitar el repudio de dichas comunicaciones» (*Ibid.*, p. 144); no obstante, en mi opinión, cuanto dice no se desprende de la firma electrónica simple o elemental a que se está refiriendo, sino, como veremos, a la firma electrónica cualificada, que se equipara, en sus efectos jurídicos, a la firma manuscrita.

[599] ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 720.

[600] No exigiéndose requisitos adicionales como los de integridad o no repudio en origen, reservados a otras clases de firma con niveles de seguridad más elevados.

[601] A diferencia de lo que sucede en nuestro país, el ordenamiento jurídico italiano alude de manera expresa a estos sistemas biométricos en el artículo 22.e) DPRDA, que, dedicado a la firma electrónica, define la clave biométrica como «[…] la sequenza di codici informatici utilizzati nell'àmbito di meccanismi di sicurezza che impiegano metodi di verifica dell'identità personale basati su specifiche caratteristiche fisiche dell'utente», o, lo que es lo mismo, «[…] la secuencia de códigos informáticos utilizados en los mecanismos de seguridad que

del nombre u otro elemento identificativo incluido al final de un mensaje electrónico, la firma manuscrita digitalizada o la existencia de una pregunta-respuesta y un PIN de acceso[602]. Resultado de lo anterior, estamos en condiciones de afirmar que, si el fin perseguido es generar certidumbre en quienes se hallen sujetos y afectados directa o indirectamente por la norma, sería más adecuado reformular el concepto actual de firma electrónica general y reconducirlo, con matices, al tradicional de firma electrónica simple, en una suerte de definición, si quiera algo más clarificadora o completa, que podría quedar como sigue: *la firma electrónica es el conjunto de datos en formato electrónico, anejos a otros datos electrónicos o asociados de manera lógica con ellos, que son utilizados, al menos, como medio de identificación del firmante*.

---

emplean métodos de verificación de la identidad personal basados en específicas características físicas del usuario»; para un estudio más profundo de la tecnología biométrica dentro del ordenamiento jurídico italiano, *vid.* MARTONI, M., *Firme elettroniche: profili informatico-giuridici*, cit., pp. 40 a 45.

[602] BUONOMO, G. Y OTROS, «La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio (alla luce delle modifiche introdotte dalla l. 221/2012)», cit., p. 15; COMANDÉ, G. Y OTROS, *Il commercio elettronico: profili giuridici*, cit., p. 102; GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, cit., p. 57; GARCÍA MÁS, F. J., «El documento público electrónico (1)», en ESCOLANO NAVARRO, J. J. (coord.) *Nuevas tecnologías en la contratación, sociedad nueva empresa e hipoteca electrónica : seminario organizado por el Consejo General del Notariado en la UIMP en julio de 2003*, Madrid, Civitas, 2005, p. 127; GONZÁLEZ DE ALAIZA CARDONA, J. J. Y OTROS, «Los contratos de adhesión y la contratación electrónica», cit., p. 1792; ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 40; PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», cit., p. 520. También, IADFE, punto 2.3.2. En concreto, existen procedimientos de firma electrónica altamente fiables que requieren de claves o contraseñas que precisan, para su obtención (normalmente en mano), de la personación física del solicitante a efectos de comprobación de la identidad; otros, en cambio, menos fiables, permiten la entrega de las mismas por medio de un procedimiento totalmente virtual, sin comprobación física de la identidad y, por ende, fácilmente accesibles por terceros. En último lugar, quedarían aquellos de tan escasa seguridad que plantean, incluso, dudas respecto de su condición de firma, dado su escaso valor probatorio a efectos de identificación o autenticación del autor (MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 74; MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», cit., pp. 226 y 227; VATTIER FUENZALIDA, C., «De nuevo sobre el régimen legal de la firma electrónica: estudio del Anteproyecto de 26 de junio de 2002», *Actualidad civil*, vol. 1, 2003, p. 140).

### 4.2. Firma electrónica avanzada

Elevando las exigencias de calidad y de seguridad de la firma electrónica, el artículo 3.11) RIE-SCTE introduce el concepto de firma electrónica avanzada, entendiendo por tal la «[…] la firma electrónica que cumple los requisitos contemplados en el artículo 26».

Estos requisitos, adiciona este último precepto, son los siguientes: a) estar vinculada al firmante de manera única[603]; b) permitir la identificación electrónica del firmante[604]; c) haber sido creada utilizando datos de creación de firma electrónica que el firmante puede utilizar para la creación de una firma electrónica, con un alto nivel de confianza[605], bajo su control

[603] La vinculación única de la firma electrónica al firmante es una consecuencia lógica del control exclusivo del firmante sobre los datos de creación de firma electrónica, determinando, por tanto, la estrecha vinculación entre los requisitos de las letras a) y d) que ahora se mencionan.

[604] Cabe plantearse si esta alusión añade algún matiz distintivo a la firma electrónica avanzada respecto de la firma electrónica simple, que, como sabemos, también permite la identificación del firmante. A favor de esta tesis, GONZÁLEZ-ECHENIQUE CASTELLANOS DE UBAO, L., «Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre firma electrónica», cit., pp. 215 y 216; con matices, CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 40, quien afirma que la seguridad conferida por la firma electrónica avanzada aparece, más bien, en el resto de los requisitos que hacen que esta firma pueda considerarse tal, en concreto, haber sido creada por medios que el firmante puede mantener bajo su exclusivo control, de forma que esté vinculada únicamente al mismo, concluyendo que «[…] poco añade a este respecto la puntualización de que la firma permita "identificar al firmante"».

[605] Con la expresión «puede utilizar, con un alto nivel de confianza», el RIE-SCTE se aproxima a la DFE y a la LFE (y se aleja del RDLFE, que eliminada toda probabilidad al respecto), algo que consideramos acertado, ya que la vinculación entre la firma y el firmante es una vinculación probable, condicionada a los medios técnicos; así también, DÍAZ MORENO, A., «Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica», cit., p. 25, que entiende este requisito como que «[…] deben existir garantías –en términos de probabilidad– de que, en ausencia de fraude o de otra conducta impropia, dos personas no pueden llegar a producir la misma firma». En consecuencia, es indudable que, bajo el actual Reglamento europeo, el titular de la firma electrónica tiene el deber de custodiar la clave privada, pero la diferencia con el RDLFE estriba en que, si efectivamente la clave privada cae en manos de un tercero, no se pierde la cualidad de firma electrónica avanzada, más allá de que esta circunstancia permita probar que un tercero y no el firmante aparente es el firmante real; se consigue así, además, una interpretación más acorde con la equivalencia entre firma manuscrita y firma electrónica, protegiéndose la apariencia de que esta última está vinculada real y exclusivamente al firmante aparente (CRUZ RIVERO,

exclusivo[606], y d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable. Obsérvese que con las tres primeras exigencias (vinculación única al signatario, identificación del mismo y creación por medios bajo su exclusivo control) se persigue garantizar la identificación autenticada del autor y evitar el rechazo en origen de los mensajes de datos; en cambio, con la última (vinculación a los datos que permite detectar cualquier alteración ulterior), se pretende salvaguardar la integridad de los documentos electrónicos[607].

Por lo demás, se conserva prácticamente la redacción que ya había caracterizado a la firma electrónica avanzada en el período de la DFE –artículo 2.2)–[608], el inmediatamente anterior

D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., pp. 55 y 56).

606 Es esto precisamente lo que persigue el artículo 11.2.a), *ab initio*, ALSEC cuando impide al PSSIisc que almacene o copie los datos de creación de firma electrónica de la persona a la que presta sus servicios. En la actualidad hay, básicamente, dos tipos de firmas electrónicas cuyos medios de creación se hallan en poder exclusivo del firmante: las firmas electrónicas biométricas y las firmas digitales de clave asimétrica, siendo estas mucho más utilizadas por la simplicidad de su funcionamiento y menor coste.

607 MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 76.

608 Sin embargo, en el artículo 2.1 PDMCSFE –COM (1998) 297 final–, se establecía un concepto de firma electrónica simple con un inciso final muy similar al que, con posterioridad, se vería recogido para la firma electrónica avanzada, añadiendo, por lo demás, una alusión a las nociones de firma digital y de signatario que luego serían suprimidas: «[…] firma en forma digital integrada en unos datos, anexa a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos: a) estar vinculada al signatario de manera única; b) permitir la identificación del signatario; c) haber sido creada por medios que el signatario puede mantener bajo su exclusivo control; d) estar vinculada a los datos relacionados de modo que se detecte cualquier alteración ulterior de los mismos». Ya en la Propuesta modificada de la Directiva todo cambia, manteniendo el artículo 2.1 la parte primera (aun modificada) para la firma electrónica general y añadiendo un artículo 2.1 bis (que en el texto definitivo se convertiría en el artículo 2.2) para una nueva clase de firma electrónica, la avanzada; así, decía el artículo 2.1, será firma electrónica (simple) «[…] los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación», siendo firma electrónica avanzada aquella comprensiva de los requisitos contenidos en las letras a) a d) anteriores. Como bien indica *Ibid.*, p. 77, «[…] esta evolución de la definición de firma electrónica supone una simplificación y flexibilización, sin duda excesiva, de la misma, pues los requisitos que inicialmente se exigían para toda firma electrónica (y, por tanto, inherentes al concepto mismo de firma), se reservan finalmente de forma única y exclusiva para las ahora denominadas firmas avanzadas (que, por otra parte, son las únicas que se benefician del reconocimiento positivo de efectos legales del art. 5.1 de la Directiva, y también del art. 3.1 del Real Decreto-ley, y del art. 3.4 de la Ley de firma electrónica, sin perjuicio

del RDLFE –artículo 2.b)[609]– y el inmediatamente posterior (reflejo de la Directiva comunitaria) de la LFE –artículo 3.2–[610]. En todas ellas, se opta por el principio de neutralidad tecnológica, más formal y aparente que real, dado que, en el fondo, el legislador nacional y comunitario, de antes y de ahora, está pensando en una modalidad tecnológica concreta, cual es la ya referida de la criptografía asimétrica de doble clave, en concreto, en el sistema de criptografía asimétrica pública del emisor o firma digital[611]. Así, la firma digital podrá ser un

---

de una "no negación" de eficacia para el resto de firmas). De forma que puede ocurrir que, dada la laxitud del art. 2.1 de la Directiva, tengan la consideración de firma electrónica procedimientos que difícilmente cumplirán la función y finalidad propias de toda firma, sea manuscrita o electrónica; con el problema de cuál sea el valor y la eficacia que haya de atribuirse a tales procedimientos (valor que se pretende salvaguardar, como veremos, en el art. 5.2 de la Directiva, y el equivalente art. 3.4 de la Ley de firma electrónica, así como, en su momento, en el art. 3.2 del Real Decreto-ley)».

609 GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, cit., p. 57. No obstante, conviene aquí hacer una precisión, ya apuntada por CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., pp. 148 y 149: bajo el RDLFE, este requisito (subsanado con la LFE, que establece el criterio contrario), relativo al dispositivo seguro de creación de firma electrónica, «[…] cubría el hecho de que el sistema de firmado digital no fuera seguro, pues la definición de firma avanzada parecía referirse al hecho de que, en realidad, el firmante fuera el único que tuviera acceso a la clave privada. Cualquiera que fuera la seguridad de la firma, si un tercero se apropiaba de la clave privada, dejaba de ser firma avanzada. Y, cualquiera que fuera la seguridad de la firma, si sólo su titular poseía la clave privada, se cumplía este requisito para ser firma avanzada, sin perjuicio de que pudiera no cumplirse algún otro requisito para que la firma electrónica equivaliera a la firma manuscrita según el artículo 3.1 Real Decreto-ley de 1999».

610 También, en Italia, al actual artículo 1.q bis) CAD, que define la firma electrónica avanzada como «[…] insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati», en castellano, «[…] conjunto de datos en forma electrónica adjuntados o conectados a un documento informático que permiten la identificación del firmante y garantizan la conexión unívoca al firmante, creados con medios sobre los que el firmante puede mantener un control exclusivo, conectados a los datos a los que dicha firma se refiere de modo que se pueda detectar si los datos mismos han sido sucesivamente modificados». Como vemos, en esta definición incorpora la noción de firma electrónica general para, a continuación, añadir aquellos requisitos que singularizan a la firma electrónica avanzada.

611 ALMONACID LAMELAS, V. Y OTROS, «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», cit., pp. 432 y 434; BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma

tipo concreto de firma electrónica avanzada cuando los datos de creación y de verificación o validación de firma electrónica empleados para crearla y para verificarla o validarla, respectivamente, adopten la modalidad de doble clave (privada y pública) propiedad del emisor del mensaje de datos, ya que, de ser así, se estaría garantizando la identificación autenticada del firmante y la integridad y no repudio en origen de dicho mensaje de datos, rasgos, estos,

---

electrónica», cit., p. 411; CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 48; DE MIGUEL ASENSIO, P. A., «Regulación de la firma electrónica: balance y perspectivas», cit., p. 4; MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., p. 133; MORENO DELGADO, M. Y OTROS, «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», cit., p. 202; ROJO GIL, F. Y OTROS, «Firma y sello electrónicos: el porqué y el cómo de la implantación del nuevo reglamento europeo», cit., p. 28. Así se pone de manifiesto por el IADFE, punto 2.3.2 (en relación con la DFE) y se infiere del análisis de algunos preceptos, como los artículos 2.4) y 7) DFE o 24.1 y 25.1 LFE, que, aun aludiendo a este sistema de cifrado con carácter enunciativo y no exhaustivo (no excluyendo, pues, el empleo de tecnologías diferentes que puedan beneficiarse de este marco normativo), parece claro que se trata de una referencia que deja claro hasta qué punto sus normas tienen en consideración la especial relevancia de la criptografía asimétrica como tecnología empleada en el sector de las firmas electrónicas, básicamente en el ámbito de las firmas electrónicas avanzadas y reconocidas. En el Reglamento eIDAS, en cambio, desaparecen estas alusiones en respuesta al otorgamiento de una renovada importancia al principio de neutralidad tecnológica (considerandos 26 y 27), que se relaciona con la rápida evolución de la tecnología y la adopción de un planteamiento abierto a innovaciones; pese a ello, se mantiene una redacción de la firma electrónica similar a la existente en la DFE, inspirada, como decimos, en el modelo de clave asimétrica como el mejor adaptado a las exigencias de las firmas electrónicas en términos de fiabilidad (DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 117 y 118). El motivo de esta orientación, añade *Ibid.*, pp. 117 y 118, responde a la falta de estándares reconocidos respecto de otras posibilidades tecnológicas, como los mecanismos de identificación biométrica, y a las limitaciones prácticas de la utilidad de su empleo en redes abiertas de otras tecnologías, como la criptografía simétrica, los números de identificación personal o la digitalización de firmas manuscritas. En cualquier caso, autores como BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 411, o MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», cit., pp. 227 y 228, sostienen que lo razonable hubiera sido que la legislación hubiera optado por centrarse en la regulación de la firma digital de manera expresa, dada la preeminencia que actualmente desempeña en la regulación del comercio electrónico, «[…] sin dejar por ello de alentar, asimismo, en el propio contenido de la norma, el recurso a otras técnicas futuras y seguras»; en la misma línea, MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 83, que advierte, en relación con la regulación por entonces propuesta, que «[…] hubiera sido más conveniente adoptar, sin duda, una posición técnica abierta, para no desalentar el recurso a otras técnicas futuras y seguras, pero excluyendo técnicas actuales inseguras, y centrándose también, y a la vez, en la regulación de la firma digital, dada la función predominante aparentemente desempeñada por la criptografía de clave pública en la práctica más reciente en materia de comercio electrónico».

propios de la firma electrónica avanzada; esta misma argumentación nos llevaría a deducir la también posible aplicación de la firma digital como modalidad específica de la firma electrónica cualificada[612], habida cuenta de que, como veremos a continuación, esta no es sino una firma electrónica avanzada dotada de mayor nivel de seguridad por la confianza que ofrecen de los elementos que la integran[613].

### 4.3. Firma electrónica cualificada

Por último, el artículo 3.12) RIE-SCTE define la firma electrónica cualificada (introduciendo una nueva denominación a nivel comunitario de aquello que, ya desde la LFE, se conocía en España como *firma electrónica reconocida*) como la «[…] firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica»[614]. De ello se desprende la existencia de toda una suerte de posibilidades diversas en materia de firma electrónica avanzada, dependiendo de los elementos con que cuente y de la seguridad que los mismos puedan llegar a imprimir (**anexo XXII**[615]).

---

[612] FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 34.

[613] A mayor abundamiento, el ordenamiento jurídico italiano vincula la firma digital exclusivamente con la firma electrónica cualificada –artículo 1.s) CAD–. No obstante, y a la vista de cuanto se ha expuesto, desconocemos por qué excluye del posible ámbito de aplicación de la firma digital a la firma electrónica avanzada.

[614] Como acabamos de indicar y como ya pusiera de manifiesto con ocasión de la LFE ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 43, al igual que la firma electrónica avanzada, la firma electrónica cualificada será, pese al criterio de neutralidad tecnológica adoptado, una auténtica firma digital, gozando, además, en este caso, de la equiparación jurídica con la firma manuscrita (principio de equivalencia funcional).

[615] En este anexo podremos observar que la firma electrónica avanzada no precisa del empleo de un certificado electrónico, más allá de que, por ser más fácil y conveniente que otros sistemas, sea habitual su empleo (ALAMILLO DOMINGO, I., «Tipología legal de la firma electrónica en la Unión Europea», cit., pp. 7 y 8; GONZÁLEZ NAVARRO, F., «Comentario al art. 45 de la Ley de régimen jurídico de las Administraciones públicas y procedimiento administrativo común», cit., pp. 31 y 33).

Este tercer y último concepto de firma electrónica, el más elevado en términos de seguridad[616], no tiene precedente en el RDLFE ni en la DFE[617], siendo introducido por primera vez en nuestro Derecho interno, repetimos, de la mano del artículo 3.3 LFE[618], que, aun con un orden inverso en su redacción, presenta el mismo contenido legal que el Reglamento eIDAS[619]. En realidad, al igual que decíamos respecto del concepto de firma digital con el

[616] DÍAZ MORENO, A., «Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica», cit., p. 5; PAFE, punto 2.

[617] No obstante, en el IADFE (punto 2.3.2) la Comisión opta ya por asignarle esta denominación, destacando los problemas encontrados para su verdadera implementación en el mercado y los nuevos impulsos que conviene adoptar: «[e]l uso de las firmas electrónicas reconocidas ha sido muy inferior al esperado y el correspondiente mercado no está aún muy desarrollado. Los usuarios no cuentan en la actualidad con un certificado electrónico único para firmar documentos o transacciones en el entorno digital, de la misma manera que en papel. Por consiguiente, no es posible hacer en este momento una valoración cabal del objetivo de la Directiva en relación con el mercado interior, a saber, la libre circulación de las firmas electrónicas reconocidas. La principal razón del lento despegue del mercado es de tipo económico: los proveedores de servicios tienen pocos incentivos para desarrollar una firma electrónica multiaplicación y prefieren ofrecer soluciones para sus propios servicios, por ejemplo, las soluciones creadas por el sector bancario. Esta situación ralentiza el proceso de desarrollo de soluciones interoperables. La falta de aplicaciones, tales como soluciones globales en materia de archivado electrónico, podría también frenar el desarrollo de una firma electrónica universal, que precisa de una masa crítica de usuarios y de usos. No obstante, en el futuro algunas aplicaciones podrían impulsar el crecimiento del mercado. El uso de la firma electrónica en los servicios de administración electrónica ha alcanzado ya cierto volumen y es probable que se convierta en un motor importante en el futuro». Y esta será, efectivamente, una de las nuevas perspectivas que adoptará el posterior RIE-SCTE al derogar la DFE, dando respuesta a la necesidad de contar con medios de identificación electrónica seguros y fomentando, al mismo tiempo, la interoperabilidad y el uso transfronterizo de la firma electrónica. En la misma línea, la SIECE –COM (2005) 229 final–, conocida como *i2010 – Una sociedad de la información europea para el crecimiento y el empleo*.

[618] Sin embargo, no se contenía en la versión primera de la norma, sí en la segunda –artículo 2.c)–, donde aparece definida como «[…] firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma», coincidiendo con la redacción posterior del artículo 3.3 LFE. En cualquier caso, como señala *Ibid.*, p. 40, no era infrecuente que, con anterioridad a la entrada en vigor de la LFE, se supliera la inexistencia del concepto de firma electrónica reconocida mediante la expresión *firma electrónica segura*, que aludía a aquella firma electrónica que reunía los requisitos del artículo 3.1 RDLFE.

[619] «Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma». En Italia, por su parte, el actualmente vigente artículo 1.r) CAD define la firma electrónica cualificada como «un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della

que se halla estrechamente ligada, se trata de una novedad más formal que real[620]; así, el apartado III de la Exposición de Motivos de la española LFE señalaba el origen, justificación y naturaleza de la firma electrónica reconocida en los siguientes términos:

> «Una de las novedades que la ley ofrece respecto del Real Decreto Ley 14/1999, es la denominación como firma electrónica reconocida de la firma electrónica que se equipara funcionalmente a la firma manuscrita. Se trata simplemente de la creación de un concepto demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio Real Decreto Ley 14/1999 venían exigiendo. Con ello se aclara que no basta con la firma electrónica avanzada para la equiparación con la firma manuscrita; es preciso que la firma electrónica avanzada esté basada en un certificado reconocido y haya sido creada por un dispositivo seguro de creación».

En consecuencia, más que una nueva modalidad, la firma electrónica cualificada constituye un nuevo tipo de firma electrónica avanzada[621] que, acompañada de determinados elementos que le imprimen una mayor seguridad (dispositivo cualificado de creación de firma electrónica –artículos 3.23) y 29 a 31 Reglamento eIDAS, artículo 24.3 LFE–, de una parte, y certificado cualificado de firma electrónica –artículos 3.15) y 28 Reglamento eIDAS, artículos 11 a 14 LFE–, de otra), tendrá «[…] un efecto jurídico equivalente al de una firma manuscrita» (artículo 25.2 RIE-SCTE)[622]. Por esta razón, se ve investida de un nuevo *nomen iuris*, con la finalidad de singularizarla de aquella otra que, por no haber sido creada mediante un dispositivo cualificado de creación de firma electrónica o por no basarse en un certificado cualificado de firma electrónica (o por no cumplir ninguno de estos dos requisitos), no tendrá efectos legales equiparables, en términos de validez y eficacia, a los de la firma autógrafa,

---

firma», es decir, «un particular tipo de firma electrónica avanzada que esté en un certificado cualificado y realizada mediante un dispositivo seguro para la creación de la firma»; su vez, como dijimos, circunscribirá la firma digital exclusivamente a «[…] un particolare tipo di firma qualificata».

620 MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., pp. 85 y 86, quien añade que la firma electrónica reconocida, «[…] más que un nuevo concepto técnico o jurídico de firma electrónica, con requisitos propios, podría ser un concepto comercial, un producto de firma electrónica»; en la misma línea, ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 42.

621 ALAMILLO DOMINGO, I., «Tipología legal de la firma electrónica en la Unión Europea», cit., pp. 9 y 10.

622 Nueva manifestación del principio de equivalencia funcional. De este modo, aclaraba en su momento *Ibid.*, p. 11, «[e]n ausencia de toda otra circunstancia, allí donde la Ley establezca el requisito de la firma o consecuencias en caso de ausencia de una firma, se podrá firmar electrónicamente».

integrándose bajo el nombre de firma electrónica avanzada[623]. Esta última, al igual que la firma electrónica simple y que la firma electrónica avanzada basada en un certificado electrónico cualificado[624], no se verá privada de efectos jurídicos ni de admisibilidad como prueba en procedimientos judiciales por el mero hecho de que esté en forma electrónica o porque no cumpla los resquisitos de la firma electrónica cualificada (artículos 25.1 RIE-SCTE y 3.9 LFE[625]), debiéndose valorar, en todo caso, cuál es la eficacia que tienen, algo que, en ocasiones, puede ser complejo y costoso[626].

Cuestión distinta, y central, es aquella que cabría plantearse al hilo de esta equivalencia entre firma electrónica cualificada y firma ológrafa: ¿no debería recibir el nombre de *firma* únicamente aquella modalidad electrónica que, por los efectos jurídicos que infiere y por las

---

[623] Antes, incluso, de su reconocimiento legal, la doctrina ya se hizo eco de esta nueva realidad; así sucede con los autores ALAMILLO DOMINGO, I./RUBIO VELÁZQUEZ, R., «Firma electrónica y certificación digital», en AA.VV. (coord.) *Internet: claves legales para la empresa*, Madrid, Civitas, 2002, pp. 636 y 637, quienes señalan que «[…] la denominación de firma electrónica reconocida se refiere a la cualificación de la calidad de la firma, de modo que no es necesario ni un contrato privado ni una norma jurídica para "reconocer" la firma».

[624] Como ya se hiciera constar en textos como el PAFE (punto 2.1), que ahora adaptamos a la nueva terminología, podremos distinguir, y así se pondrá de manifiesto claramente en el texto del RIE-SCTE, tres tipos de firmas electrónicas avanzadas: la firma electrónica avanzada propiamente dicha (que será aquella firma electrónica avanzada que no ha sido creada mediante un dispositivo cualificado de creación de firma electrónica y que no está basada en un certificado cualificado de firma electrónica), la firma electrónica avanzada basada en un certificado cualificado de firma electrónica (pero no creada mediante un dispositivo cualificado de creación de firma electrónica) y la firma electrónica cualificada (que es aquella firma electrónica avanzada que ha sido creada mediante un dispositivo cualificado de creación de firma electrónica y que está basada en un certificado cualificado de firma electrónica).

[625] Antes de la LFE, artículo 3.2 RDLFE, cuya redacción, subraya VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., p. 148, «[…] fue criticada por la doctrina, dado que el tenor del texto no resultaba acertado, pues una cosa es la posibilidad de que un documento pueda ser admitido en juicio como prueba, y otra muy distinta es que se le dote de eficacia probatoria»; sobre esta cuestión, *vid.* GONZÁLEZ-ECHENIQUE CASTELLANOS DE UBAO, L., «La firma electrónica», en AA.VV. (coord.) *Derecho de Internet: la Ley de servicios de la sociedad de la información y de comercio electrónico*, Cizur Menor, Aranzadi, 2003, p. 625.

[626] Así, como bien señala ALAMILLO DOMINGO, I., «Los servicios de confianza y la prueba electrónica», cit., p. 148, «[…] en aplicación de los principios de equivalencia funcional, una firma electrónica puede ser equivalente a una firma manuscrita, diferenciándose la firma electrónica cualificada de las demás porque la misma es claramente equivalente a la firma manuscrita, por mandato legal, mientras que en las restantes firmas electrónicas eventualmente se deberá probar su idoneidad, en función del caso concreto».

exigencias que satisface respecto al autor del documento y al contenido mismo de este, es la única equiparable a la firma manuscrita? Entiendo que sí, pues, de lo contrario, nos estaremos encontrando (y así sucede en la actualidad) con una situación del todo paradójica, derivada de atribuir la denominación de firma a modalidades (como serán, en su caso, la firma electrónica simple y la firma electrónica avanzada) que no cumplan con la precitada equiparación. En consecuencia, toda aquella modalidad de lo que ahora conocemos como firma electrónica que no goce finalmente de esta equivalencia, no podría, a fin de evitar confusiones en nada convenientes, tener la consideración de firma; y no podría, no porque no consista en un trazo autógrafo en soporte físico papel (a estas alturas, parece evidente, ningún tipo de firma electrónica responde a estas características), sino porque no cumple, como mínimo, las funciones tradicionalmente desempeñadas por la firma manuscrita.

Por lo demás, esta equivalencia con la firma manuscrita, plasmada en nuestro país por primera vez en el artículo 3.4 LFE[627], ya estaba recogida con carácter previo en el artículo 3.1 RDLFE, que disponía lo que sigue:

---

[627] «[…] La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel». En el Derecho italiano, el artículo 10.3 DPRDA, modificado por el artículo 6 DLDFE, aun sin mencionar expresamente esta equiparación entre firma electrónica reconocida y firma manuscrita, sí que establece que aquella hará prueba plena de su existencia, y lo hace en los siguientes términos: «[i]l documento informatico, quando è sottoscritto con firma digitale o con un altro tipo di firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto», en castellano, «[e]l documento informático, cuando está suscrito con firma digital o con otro tipo de firma electrónica avanzada, y la firma está basada en un certificado cualificado y es generada mediante un dispositivo para la creación de una firma segura, hace además prueba plena, salvo querella de falsedad, de la procedencia de las declaraciones del que la ha suscrito». En este sentido, algún autor como BUONOMO, G., «Lo schema governativo stravolge il processo civile», *InterLex*, vol. 1, 2002, p. 1, ha optado por considerar que del precitado artículo se desprende que el documento electrónico con firma digital es equivalente a la firma auténtica de notario; en contra, en cambio, CAMMARATA, M./MACCARONE, E., *La firma digitale sicura. Il documento informatico nell'ordinamento italiano*, Milán, Giuffrè, 2003, p. 93, quienes subrayan los efectos altamente perniciosos que supondría adoptar la decisión anterior. En la actualidad, la norma anterior se ha visto derogada por el artículo 21 CAD, que, en sus apartados 1 y 2, sostiene que «1. [i]l documento informatico, cui è apposta una firma elettronica, soddisfa il requisito della forma scritta e sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. 2. Il documento informatico sottoscritto con firma elettronica avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche di cui all'articolo 20, comma 3, ha

«La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba en juicio, valorándose ésta según los criterios de apreciación establecidos en las normas procesales. Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21»[628].

---

altresì l'efficacia prevista dall'articolo 2702 del codice civile. L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria. Restano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa anche regolamentare in materia di processo telematico», es decir, «1. [e]l documento informático, sobre el que se coloque una firma electrónica, satisface el requisito de la forma escrita y sobre el plano probatorio es libremente valorable en juicio, teniendo en cuenta sus características objetivas de calidad, seguridad, integridad e inmodificabilidad. 2. El documento informático firmado con firma electrónica avanzada, cualificada o digital, formado en el respeto de las reglas técnicas del artículo 20.3, tiene asimismo la eficacia prevista en el artículo 2702 del Código civil. El empleo del dispositivo de firma electrónica cualificada o digital se presume atribuible al titular, salvo prueba en contrario. Se mantienen las disposiciones concernientes al depósito de los actos y de los documentos por vía telemática según la normativa también reglamentaria en materia de proceso telemático».

[628] Sin embargo, desde entonces, la redacción de la norma fue criticada por adolecer de uno de los elementos fundamentales para el desarrollo de los intercambios telemáticos, como es el necesario reconocimiento de esta modalidad superior de firma electrónica por todos los operadores en el tráfico jurídico, tanto públicos como privados. Así sucede con ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., pp. 26 a 30, quienes sostienen que «[u]na vez cumplidos los requisitos técnicos que permiten la consideración de una firma electrónica como reconocida, resulta desconcertante que no se ampare a esa firma dotándola no sólo de la equiparación con la firma manuscrita, sino también estableciendo la obligatoria aceptación y reconocimiento de la misma en todos aquellos actos o negocios jurídicos en que intervenga. Una regulación moderna ha de intentar que esta problemática quede superada, permitiendo la utilización de los medios telemáticos que gocen del más alto nivel de seguridad en el más amplio círculo posible. Y esto sólo será posible a través de la imposición a los diferentes sujetos que intervienen en el tráfico jurídico, ya sean públicos o privados, de la obligatoria admisión de la firma electrónica (evidentemente habrá de ser la reconocida) en las operaciones en que intervienen. Evidentemente, esta obligatoriedad sólo puede imponerse por una norma con rango de ley y, tratándose del ámbito del Derecho Privado, el Código Civil es la norma más apropiada para recoger esa imposición, junto a una declaración de carácter general de necesaria aceptación de la firma electrónica». Para ello, se propusieron varias medidas, como la incorporación de un apartado como el que sigue: «[l]a firma electrónica reconocida será aceptada por todas las personas físicas y jurídicas sujetas a esta Ley, siempre que dicha aceptación resulte técnica y operativamente posible y la firma electrónica reconocida

También a nivel comunitario, en el artículo 5.1 DFE:

> «Los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma: a) satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel; y b) sea admisible como prueba en procedimientos judiciales».

## III. EFECTOS LEGALES DE LA FIRMA ELECTRÓNICA

Entre las principales funciones de la firma electrónica en el campo estricto de la contratación *online* se halla la de identificar a los sujetos participantes, además de asegurar de modo fehaciente que todas y cada una de las comunicaciones que transitan virtualmente resultan son realizadas de forma íntegra y voluntaria y accesibles tan sólo por quienes son sus respectivos emisores y destinatarios[629]. Para la atribución de todos o algunos de los efectos anteriores, suelen distinguirse dos aspectos fundamentales en torno a la validez y eficacia de la firma electrónica, que analizaremos por separado para una mejor comprensión: de un lado, los aspectos materiales, determinados por los efectos jurídicos específicos que, para cada tipo o modalidad de firma electrónica, prevé la norma; de otro lado, los aspectos puramente procesales, que regulan el *íter* a seguir para el caso de que se impugne su autenticidad, donde tendremos que tener en cuenta el controvertido valor probatorio del documento en el que la firma electrónica haya, en su caso, de insertarse.

---

haya sido verificada»; la (en mi opinión, verdaderamente adecuada para la consecución del principio de equivalencia funcional, en modo similar al artículo 23.3 LSSICE para los contratos electrónicos) modificación del CC, introduciendo un artículo 1279 bis, que tendría la siguiente redacción «1. Cuando la ley española requiera de forma imperativa la firma escrita, toda persona física o jurídica podrá emplear su firma electrónica reconocida para cumplir dicho requisito. 2. Cuando la ley española requiera de forma dispositiva la firma escrita, toda persona física o jurídica podrá emplear cualquier firma electrónica para cumplir dicho requisito», o, en el caso de las Administraciones públicas, «[e]l empleo, siempre que sea posible, de la firma electrónica reconocida, con las adaptaciones que, sin afectar a la compatibilidad de los sistemas, sean necesarias en cada Administración Pública».

[629] MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., pp. 166 y 167.

1. Aspectos materiales

En este punto, y por ser distintos los efectos jurídicos previstos para la firma electrónica cualificada, de un lado, y para aquellas otras que no ostenten el mismo nivel de seguridad, de otro, se hace preciso realizar la siguiente distinción.

1.1. Firma electrónica cualificada: equivalencia funcional con la firma manuscrita y equiparación a nivel comunitario

La firma autógrafa, en lo que aquí nos interesa, es la forma habitual de vincular un documento a una persona concreta, mostrando con su plasmación a quien sea su receptor que el documento y la declaración contenida en el mismo se dan por concluidos y se asumen como propios[630]. Sobre estos parámetros, la firma tiene claramente una función probatoria, toda vez que el signo manuscrito en que consiste formalmente es fundamental para preconstituir, desde el momento justo en que se documenta la declaración, el objeto de la prueba caligráfica, prueba que, en sede judicial, podrá fijar con gran probabilidad la autoría del signo y, con ello, de la declaración[631].

Pese a ello, la firma manuscrita no aparece definida en nuestro ordenamiento jurídico[632]; el legislador da por supuesto este concepto, limitándose a invocar su existencia como medio

[630] CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 19. Obviamente, también existirán casos en los que la declaración plasmada en el documento a través de la firma no tenga por objeto propio el de asumir los efectos del acto jurídico documentado, sino tan sólo una declaración instrumental respecto al mismo; entre estos supuestos, el autor cita la firma de testigos, «[…] cuya declaración puede reducirse a indicar su presencia física bajo la condición de tales» (*Ibid.*, p. 19).

[631] En este sentido, la STS núm. 356/2003, de 3 de abril, F. J. 2º, dispone que es doctrina constante del TS que «[…] acreditada por cualquiera de los referidos medios la autenticidad de la firma que autoriza un documento privado, se reputa veraz y exacto su contenido, a menos que se pruebe y hasta tanto se demuestre la existencia de hechos que permitan desvirtuar tal consecuencia (Sentencia de 5 de mayo de 1958 y 20 de febrero de 1978). Dada la escritura mecanográfica, la prueba documental se transmuta en caligráfica sobre la firma del documento, por constituir reiterada doctrina jurisprudencial de que existe la presunción "iuris tantum" de [que] quien firma un documento conoce y admite su total contenido, salvo que pruebe lo contrario (Sentencia de 2 de octubre de 1980)».

[632] La RAE define la firma manuscrita como el «[r]asgo o conjunto de rasgos, realizados siempre de la misma manera, que identifican a una persona y sustituyen a su nombre y apellidos para aprobar o dar autenticidad a

de prueba en el CC y en la LECiv, al tiempo que alude, en muy contadas ocasiones, a los escritos firmados como modo de documentar diversos actos jurídicos.

Pues bien, el artículo 25.2 Reglamento eIDAS dispone que «[u]na firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita»[633]. De nuevo, vuelve a manifestarse con fuerza el principio de equivalencia funcional, propio del Derecho de la contratación electrónica, que persigue, con las adaptaciones propias y oportunas del nuevo (y complementario) medio en el que, cada vez con más insistencia, se desenvuelven las relaciones sociales y económicas, atribuir, en la medida de lo posible, las mismas consecuencias

un documento». Jurisprudencialmente, la firma manuscrita fue definida por la STS de 3 de noviembre de 1997, F. J. 10º como «[…] el 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 con lo que en ellos se dice. Aunque la firma puede quedar reducida, sólo, a la rúbrica o consistir, exclusivamente, incluso, en otro trazado gráfico, o en iniciales, o en grafismos ilegibles, lo que la distingue es su habitualidad, como elemento vinculante de esa grafía o signo de su autor»; no obstante, indica la misma sentencia, «[…] la firma autógrafa no es la única manera de signar, pues hay otros mecanismos que, sin ser firma autógrafa, constituyen trazados gráficos, que asimismo conceden autoría y obligan. Así, las claves, los códigos, los signos y, en casos, los sellos con firmas en el sentido indicado». Por último, afirma también que «[…] el requisito de la firma autógrafa o equivalente puede ser sustituida, por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfanuméricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido». Desde una perspectiva puramente doctrinal, ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 36, define la firma en sentido general como «[…] el signo único que una persona realiza con el fin de identificarse y de asumir el acto que signa», de modo que, continúa, «[…] la finalidad perseguida, al firmar un documento, es doble: a) asumir la autoría del mismo y b) adquirir los derechos y obligaciones que de éste se desprendan». De acuerdo con este autor, son cinco las condiciones básicas que, en la práctica, ha de cumplir la firma manuscrita para poder gozar de eficacia jurídica en nuestro ordenamiento jurídico: 1) que el documento esté escrito con tinta indeleble y en soporte papel absorbente, de tal modo que una corrección o una alteración posterior, que altere el contenido, sea visible y evidente; 2) que el documento esté comprendido en márgenes razonables que contengan los renglones escritos, de tal forma que cualquier modificación posterior sea apreciable de forma evidente; 3) que la firma manuscrita cierre la información escrita, no pudiéndose incluir información adicional salvo después de la firma; 4) que el firmante use siempre la misma firma manuscrita en todos los documentos asumidos, y 5) que la firma manuscrita contenga un razonable grado de dificultad que haga altamente difícil su falsificación.

[633] Fuera de nuestras fronteras, dispone el ordenamiento jurídico italiano que «[l]'apposizione di firma digitale integra e sostituisce l'apposizione di sigilli, punzoni, timbri, contrassegni e marchi di qualsiasi genere ad ogni fine previsto dalla normativa vigente», es decir, «la plasmación de una firma digital integra y reemplaza la plasmación de sellos, punzones, cuños, marcas comerciales y marcas de cualquier tipo a los efectos previstos por la normativa vigente» (artículo 24.2 CAD).

jurídicas a uno y otro entorno, el físico y el virtual[634]. En consecuencia, para su plena operatividad y, por ende, para la consecución de la correspondencia prevista en el precepto, tan sólo será necesario que la firma electrónica cumpla todos y cada uno de los requisitos necesarios para tener la consideración de firma electrónica cualificada (pudiendo ello acreditarse con la validación del artículo 32 RIE-SCTE). No obstante, en ocasiones (especialmente en caso de impugnación), este aspecto puede requerir de dificultosos informes técnicos que permitan demostrar ante el juez la existencia de tales requisitos, siendo, con frecuencia, prácticamente imposible su prueba o constancia[635].

---

[634] No obstante, en un estricto plano teórico, esta equiparación ha suscitado cierta controversia sobre la base de la génesis del concepto de *seguridad*, inherente a toda la legislación comunitaria y nacional; así, autores como RECODER DE CASSO, E., «Algunas observaciones en torno a contratos, electrónica y fe pública», en DE ROS CEREZO, R. M./CENDOYA MÉNDEZ DE VIGO, J. M. (coords.) *Derecho de Internet : la contratación electrónica y firma digital*, Cizur Menor, Aranzadi, 2000, p. 120, sostienen que una cosa es la seguridad técnica y otra la seguridad jurídica, ya que «[…] no es lo mismo prestar consentimiento mediante la firma con las implicaciones que eso conlleva, que cuestionarse si la tinta es de mejor o peor calidad o si es más fácil o difícilmente falsificable», poniendo de relieve su sorpresa por el otorgamiento de efectos jurídicos privilegiados por el mero hecho de que la firma sea realizada por medio de un sistema que imposibilite su alteración, «[…] pues lo que aporta seguridad al sistema jurídico […] de unos efectos privilegiados a la firma, es la autenticidad del documento, y esta autenticidad, insisto, no se logra por el hecho de que la tinta sea de mejor o peor calidad ni porque el programa informático sea más o menos fiable. Se logra por la interposición del consentimiento y eso es precisamente lo que dispone nuestro ordenamiento jurídico». No obstante, estoy de acuerdo con ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 58, cuando afirma que «[…] en el campo de la nueva contratación electrónica mediante redes, esta concepción, simplemente, es irreal. Si bien es cierto que ambos conceptos (seguridad jurídica y seguridad técnica) pueden ser diferenciados claramente en algunas actividades, en la moderna contratación electrónica la separación radical de ambos conceptos es imposible. No son conceptos aislados. La seguridad técnica impacta en la seguridad jurídica y, en este ámbito, la segunda se torna imposible sin la primera. De no existir una solución técnica como la firma electrónica, y no poder beneficiarnos de las funciones jurídicas que nos reporta, la seguridad jurídica sería imposible. Es cierto que la autenticidad del consentimiento es piedra angular de ésta pero, por un lado, en el empleo de la firma electrónica los pilares generales de la contratación permanecen inmutables incluido el consentimiento, y por otro, el soporte y el medio –seguridad tecnológica– mediante el cual se plasma esa declaración volitiva afecta directamente y decisivamente a la seguridad jurídica. En ese sentido, plantear si "la tinta es de mejor o peor calidad o si el programa es más o menos fiable", sí parece acertado, pues si bien de ella no depende la autenticidad del consentimiento es evidente que disminuimos el riesgo de falsificación y por tanto, favorecemos su autenticidad» (los paréntesis son propios).

[635] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 90.

Sin variaciones sustanciales, esta regla ya se contenía a nivel europeo en el artículo 5.1.a) DFE, que disponía lo que sigue:

> «Los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma: a) satisfaga el requisito jurídico de una firma en relación con los datos en forma electrónica del mismo modo que una firma manuscrita satisface dichos requisitos en relación con los datos en papel»[636].

También a nivel nacional, el artículo 3.1, *ab initio*, RDLFE, antes incluso de la Directiva comunitaria, vino a afirmar que:

> «La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel».

No obstante, para evitar las dificultades de acreditación del cumplimiento de los requisitos de equiparación, introduce un párrafo segundo al apartado primero que dispone, literalmente, que:

> «Se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicados en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21».

Con ello, se establecía una presunción de cumplimiento de los requisitos necesarios para la equivalencia funcional con la firma manuscrita ligada a la satisfacción de otras exigencias complementarias: certificado reconocido emitido por un PSSIic y dispositivo seguro de creación de firma electrónica certificado[637].

---

[636] Que recoge el principio de equivalencia funcional recogido posteriormente en el considerando 34 y en el artículo 9.1 DCE, así como en el apartado IV y en el artículo 23, apartados 1 y 3, LSSICE, para los contratos electrónicos.

[637] MARTÍNEZ NADAL, A., «Firma electrónica», cit., p. 197; MARTÍNEZ NADAL, A., «La ley española de firma electrónica (Real Decreto Ley 14/1999)», cit., p. 111.

Después, el artículo 3.4 LFE, tan sólo con la modificación formal derivada de la introducción del concepto de firma electrónica reconocida, afirma categóricamente que «[l]a firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel». Sin embargo, desaparece aquí la presunción legal del artículo 3.1.2º RDLFE; y desaparece no sólo implícitamente en este artículo 3 LFE, sino también en virtud de un pronunciamiento expreso del artículo 26.4 LFE, que dispone que «[l]a certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia jurídica a una firma electrónica». Se cumple, de esta manera, aquello que ya anunciaba la Exposición de Motivos en los siguientes términos:

> «Por otra parte, la ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y *eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la Directiva*. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación»[638].

En este sentido, como bien señala MARTÍNEZ NADAL[639], «[…] la eliminación de esta presunción probablemente sea consecuencia lógica e inevitable de la tendencia a la privatización de los sistemas de certificación, ya que no siempre tendría fundamento la atribución de efectos legales de tal trascendencia como los contenidos en la presunción del art. 3 RDL a una simple declaración de una entidad de naturaleza privada; además del problema de la convivencia de sistemas públicos y privados de certificación, e incluso, dentro de éstos, de sistemas privados de distinto contenido, seguridad y fiabilidad, con las consiguientes dudas sobre a cuál de estos distintos sistemas beneficiaría la presunción legal».

La duda que surge de manera inmediata en estos casos es qué sucede si no intervienen estos procesos de certificación. *A priori*, la producción de efectos jurídicos en el tráfico es idéntica, de modo que, exista o no certificación del PSSIic y del dispositivo de creación de

[638] La cursiva es propia.

[639] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 92.

firma electrónica, si esta cumple los requisitos del artículo 3.3 LFE, será reconocida[640]. Ahora bien, no es menos cierto que la intervención de estos procesos certificadores puede resultar esencial en el caso en el que se impugne una firma electrónica reconocida; en efecto, dos pueden ser las ventajas fundamentales que lleven al PSSIic a solicitar esta certificación: de un lado, generar la confianza necesaria del mercado en los productos de firma electrónica que ofrece a través de la exhibición de la certificación como sello de calidad, mayor cuanto mayor sea la fiabilidad que genere la entidad certificadora[641]; de otro, que, a través de la certificación, pueda probarse el cumplimiento de las obligaciones que deben ser objeto de comprobación al impugnarse la firma electrónica reconocida[642].

Hasta aquí, todo igual. No obstante, el artículo 25.3 del Reglamento sí que incorpora una novedad respecto del cuerpo normativo anterior, al añadir explícitamente una propiedad adicional a las firmas electrónicas creadas por dispositivos cualificados y basadas en certificados cualificados. Esta propiedad es la de la equiparación comunitaria de firmas electrónicas cualificadas, firmas que, surgidas en cualquier Estado miembro, habrán de ser reconocidas como tales en todos los demás[643]. Algo parecido disponía la DFE en su artículo 4.2, al establecer, refiriéndose a los productos de firma electrónica (no a la firma electrónica propiamente dicha) y sin concretar a qué tipo de firma electrónica estaba aludiendo, que «[l]os Estados miembros velarán por que los productos de firma electrónica[644] que se ajusten a lo dispuesto en la presente Directiva puedan circular libremente en el mercado interior», reforzando, de

---

[640] ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 63.

[641] GÓMEZ DE LIAÑO GONZÁLEZ, F., *El proceso civil*, cit., p. 467.

[642] ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., p. 65.

[643] Cae la redacción de este apartado, sin embargo, en una redundancia ciertamente innecesaria, pues, al hablar de «[u]na firma electrónica cualificada basada en un certificado cualificado», parece dar a entender (erróneamente) que cabe la posibilidad de que existan firmas electrónicas cualificadas que no estén basadas en certificados cualificados; además, da por hecho algo que, si se opta (como parece hacer aquí) por la minuciosidad, debería haberse introducido, como es la necesidad de que sean creadas por medio de dispositivos cualificados de creación firma electrónica, la segunda de las características necesarias que ha de reunir este tipo de firma electrónica para ser jurídicamente considerada como tal.

[644] Definidos en el artículo 2.12) DFE como los programas o materiales informáticos, o sus componentes específicos, que se destinan a ser utilizados por el PSSIic para la prestación de servicios de firma electrónica o para la creación o verificación de firmas electrónicas.

este modo, el principio de libre circulación dentro del mercado interior, distinto del principio de reconocimiento mutuo a que ahora nos referimos[645].

### 1.2. Firmas electrónicas no cualificadas

Bien podemos advertir, a la vista de lo anterior, la configuración de la firma electrónica cualificada como aquella modalidad dotada de las máximas garantías técnicas de seguridad, fiabilidad y reconocimiento por terceros, constancia esta que lleva a atribuirle la máxima eficacia jurídica: la equiparación formal y funcional con la firma manuscrita. Sin embargo, cabría preguntarse qué sucede con aquellas otras modalidades de firma electrónica que no gozan de este reconocimiento pleno.

En este sentido, el artículo 25.1 RIE-SCTE dispone que no se denegarán efectos jurídicos (si bien, parece obvio que estos no serán los mismos que los que previstos para las firmas electrónicas cualificadas) a una firma electrónica (no cualificada, se sobreentiende) por el mero hecho de ser una firma electrónica (y no una firma manuscrita) o porque no cumpla los requisitos de la firma electrónica cualificada (y se trate, pues, de una firma electrónica simple o de una firma electrónica avanzada). En consecuencia, mientras que la firma electrónica cualificada cuenta con unos efectos legalmente determinados (repetimos, equivalencia legal con la firma manuscrita), toda firma electrónica que no sea cualificada podrá gozar (o no) de efectos jurídicos específicos respecto de la autoría, integridad, confidencialidad o no rechazo del documento electrónico[646], si bien, por razones obvias, no resultará posible determinar cuáles de estos efectos con carácter apriorístico, debiendo valorarse atendiendo a cada supuesto en concreto, valoración esta que, dependiendo del caso, puede ser compleja y costosa[647].

---

[645] En todo caso, aclaraba el PAFE, «[l]a aceptación transfronteriza de la firma electrónica sólo se aplica, no obstante, al nivel reconocido, ya que el artículo 4, apartado 2, establece la libre circulación de los productos de firma electrónica que se ajustan a lo dispuesto en la Directiva (lo cual en la práctica significa ajustarse a los requisitos establecidos en los anexos de la misma para las firmas electrónicas)».

[646] ALMONACID LAMELAS, V. Y OTROS, «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», cit., p. 433.

[647] MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», cit., p. 229.

Esta misma previsión fue acogida por el artículo 5.2 DFE, que, por no incluir a la firma electrónica reconocida como tal, resultaba tanto más detallado en su redacción:

> «Los Estados miembros velarán por que no se niegue eficacia jurídica […] a la firma electrónica por el mero hecho de que: ésta se presente en forma electrónica, o no se base en un certificado reconocido, o no se base en un certificado expedido por un proveedor de servicios de certificación acreditado[648], o no esté creada por un dispositivo seguro de creación de firma».

Y así se refleja en el artículo 3.9 LFE que, reemplazando al artículo 3.2 RDLFE, dispone que «[n]o se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica»[649]. No obstante, en este caso la redacción es, en mi opinión, inadecuada por confusa o por desubicada, y así podemos constatarlo gracias al análisis posterior del artículo 25.1 RIE-SCTE; en efecto, de este último precepto podemos concluir (apartado primero) que no podrán negarse efectos jurídicos a la firma electrónica por el mero hecho de que (a) sea tal (de modo que reconoce la posible validez de toda firma electrónica, ya sea simple, avanzada o cualificada) *o* porque (b) no cumplan los requisitos más elevados de las firmas electrónicas cualificadas (de modo que reconoce la posible validez de toda firma electrónica que sea simple o avanzada), reconociendo a continuación (apartado segundo) el efecto jurídico propio y específico de la firma electrónica cualificada. En cambio, de la sola lectura aislada de la LFE podríamos llegar a inferir que ambos requisitos deben darse cumulativamente, de suerte que no podrán negarse efectos jurídicos tan sólo a aquellas firmas electrónicas que, no cumpliendo los requisitos de una firma electrónica reconocida, conste en forma electrónica, afectando únicamente a las firmas electrónicas simple y avanzada y no incluyendo en esta prohibición general a la firma electrónica reconocida. Cierto es

---

[648] Punto, este, innecesario y confuso, ya que con el anterior y el posterior se da por hecho que no estaríamos en presencia de una firma electrónica reconocida, de modo que la firma electrónica resultante (fuese simple, fuese avanzada) no podría gozar del reconocimiento que a aquella se anuda.

[649] Ya en esa época, ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 31, advertían de lo conveniente de añadir al texto de la LFE la obligación de regular el uso de las firmas electrónicas que no fueran reconocidas, en una redacción que podría ser como la propuesta por ellos mismos: «[l]as personas físicas y jurídicas que empleen la firma electrónica que no reúna los requisitos de la firma electrónica reconocida deberán regular, mediante el instrumento jurídico apropiado, las condiciones jurídicas, técnicas, organizativas y de seguridad aplicables a la generación, verificación y, en su caso, archivo, de la firma electrónica».

que, previamente (apartado 4), reconoce el efecto jurídico que tendrá la firma electrónica reconocida, ampliando, por tanto (si bien de manera implícita), este eventual reconocimiento general de efectos a toda firma electrónica; sin embargo, lo lógico hubiera sido incluir inicialmente todos los tipos de firma electrónica o, de optar por esta redacción, introducir este apartado 9 antes que el apartado 4, infiriendo al artículo 3 una estructura algo más lógica y coherente.

### 1.3. Reconocimiento de la autonomía de la voluntad de las partes

Parece necesario poner de relieve en este momento la admisibilidad y la plena operatividad que la ley otorga a la (por algunos autores[650]) denominada *firma electrónica convencional*, aceptada implícitamente por el artículo 2.2 RIE-SCTE. De acuerdo con este precepto, «[e]l presente Reglamento no se aplica a la prestación de servicios de confianza utilizados exclusivamente dentro de sistemas cerrados resultantes del Derecho nacional o de acuerdos entre un conjunto definido de participantes».

Esta previsión ya venía plasmada en nuestro Derecho interno desde la entrada en vigor de la LFE, cuyo artículo 3.10 disponía expresamente que «[a] los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas»[651]. Así, y en virtud del principio de autonomía de la voluntad, las partes serán libres de fijar las condiciones que hayan de regir en el uso de la firma electrónica *inter partes*[652], más allá de cuanto

---

[650] ALAMILLO DOMINGO, I. Y OTROS, «Firma electrónica y certificación digital», cit., p. 641; GÁLLEGO HIGUERAS, G. F., «Comentarios a la reciente Ley 59/2003, de 19 de diciembre, de firma electrónica: algunas novedades al marco regulador existente», cit., p. 25.

[651] El origen de este precepto viene anunciado en el considerando 16 de la DFE, que dispone lo siguiente: «[l]a presente Directiva contribuye al uso y al reconocimiento legal de la firma electrónica en la Comunidad; no se precisa un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado celebrados entre un número determinado de participantes. En la medida en que lo permita la legislación nacional, ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas; no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales».

[652] Estas condiciones, señalan RUBIO VELÁZQUEZ, R. Y OTROS, *La firma electrónica: aspectos legales y técnicos*, cit., pp. 38 y 39, «[…] podrán tener en cuenta, entre otros, los siguientes aspectos: 1. Selección del ámbito de uso

disponga la norma, que no será de aplicación en estos supuestos salvo de modo subsidiario, rigiendo los términos establecidos en el contenido del acuerdo. Pese a ello, no faltan autores[653] que han puesto de manifiesto el peligro de esta previsión, especialmente en aquellos supuestos en que de la fijación de los términos de funcionamiento de la firma electrónica por las partes se derive una situación de desigualdad entre ellas; no obstante, de no incurrir en problemas de este tipo, lo cierto es que, amoldadas a las necesidades de las partes (que pueden requerir de aspectos no contemplados o distintos de los contemplados legalmente), pueden resultar positivas para obtener una respuesta más satisfactoria a sus necesidades particulares[654].

## 2. Aspectos procesales

En este otro apartado, por su parte, ponemos el énfasis en aquellas importantes cuestiones de naturaleza procesal relacionadas con la firma electrónica. Veamos con detenimiento cuáles son.

### 2.1. Documento electrónico: el problema de la antinomia legislativa en materia de prueba

Ya tuvimos ocasión de analizar la figura general del documento al inicio del capítulo precedente, así como las distintas teorías existentes en torno a ella. Fue en ese momento cuando, superando la confusión terminológica imperante, distinguimos claramente entre documento tradicional o contenido escrito archivado en soporte físico papel y documento electrónico o contenido escrito, visual o auditivo archivado en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica. Al tiempo, aportábamos una defi-

---

de la firma electrónica. 2. Determinación del significado exacto del acto de firma, atribuyéndole un valor concreto, no necesariamente como autor del documento, sino como revisor, testigo, etc. 3. Establecimiento de la necesidad de emplear ciertos atributos y de la fuente de obtención de los mismos, tales como poderes, autorizaciones, roles, cargos, etc. 4. Necesidad de emplear ciertos mecanismos de verificación de los certificados reconocidos, como listas de certificados revocados (CRLs). 5. Establecimiento de ciertos requisitos adicionales para considerar válida una firma electrónica entre las partes. Estos requisitos pueden ser técnicos, funcionales o subjetivos. 6. Establecimiento de efectos adicionales a los previstos por la ley para el tipo de firma empleada».

653 Entre otros, GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, cit., p. 69.

654 En esta línea, MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 81.

nición particular de documento que, con vocación globalizadora de cuantos fenómenos similares a los actualmente existentes pudieran suscitarse en el futuro, quedaba redactada como sigue: *contenido almacenado en un soporte físico en papel u otro material adecuado que proporciona información, escrita, vista o hablada, fidedigna o relevante sobre hechos con eficacia probatoria o cualquier otro tipo de utilidad jurídica.*

Pues bien, en esta descripción general de documento quedaría perfectamente incluida la noción de documento electrónico[655], definido por primera vez en nuestro ordenamiento jurídico interno en el artículo 3.5 LFE y por primera vez a nivel comunitario en el artículo 3.35) RIE-SCTE. Ahora bien, mientras que el primero de los preceptos anteriores incurre en el error, tantas veces apuntado, de confundir los términos *soporte* (que, aun en el caso del documento electrónico, ha de ser físico) y *material de ese soporte* (que en el caso del documento tradicional será el papel, mientras que en el caso del documento electrónico será uno distinto del papel pero apto para el archivo de información de naturaleza electrónica)[656], este segundo

[655] A favor de la naturaleza documental del documento electrónico se encuentra, entre otros, RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., pp. 14 y 15, quien se expresa en los siguientes términos: «[…] la naturaleza documental del documento electrónico me parece indudable. El documento no puede definirse solamente por su contenido, como la "expresión de un pensamiento humano con relevancia jurídica", pues no se distinguiría entonces en su función probatoria, procesal y extraprocesal, de las declaraciones de partes y testigos, ni en su función dispositiva, de los otros medios de manifestación del pensamiento y de la voluntad de los hombres, como la palabra y los hechos concluyentes; su esencia se encuentra en las características del vehículo de esa expresión, el verificarse "por medio de una cosa a la que un hombre ha incorporado unos signos" que la hacen apta para ello; en sus notas de "real" y "artificial". El documento es, pues, según IRTI, una *res signata*, una cosa signada, en que ambos elementos son imprescindibles: "el documento no es la cosa, ni es el signo sino conjuntamente *res signata*, objeto sobre el cual el hombre ha obrado". El documento se nos presenta así como una *cosa*, una realidad del mundo exterior, constituida por una materia y una grafía artificialmente incorporada a ella. La *materia documental* era hasta ahora casi exclusivamente el papel; pero históricamente habían sido utilizados el ladrillo cocido, las tablas de madera enceradas, el papiro, el pergamino, etc., y de ello fácilmente puede deducirse la accidentalidad de la materia "papel" y la posibilidad del documento sinpapel (*paperless*). Se impone pues un indiferentismo respecto de la materia documental, ya formulado para el testamento en el Derecho romano y en el de Partidas, en virtud del cual se acepta para la corporalidad del documento cualquier materia apta como vehículo de expresión del pensamiento humano [...]. La materia de la que se va a formar el documento puede, en efecto, ser tan variada como permitan los adelantos de la técnica y de la industria, por lo que en principio se deben admitir los llamados documentos electrónicos como verdaderos documentos».

[656] Recordemos, «[…] información de cualquier naturaleza en forma electrónica, archivada *en un soporte electrónico* según un formato determinado y susceptible de identificación y tratamiento diferenciado» (la cursiva es propia).

lo supera, quien sabe si por su simplicidad, limitándose a establecer que por documento electrónico se entenderá «[…] todo contenido almacenado *en formato electrónico*[657], en particular, texto o registro sonoro, visual o audiovisual»[658], coincidiendo con cuanto quedó reflejado en el **anexo IX** del presente estudio al hablar de una nueva teoría, propia, que identifica el documento con el contenido y no con el continente.

Así lo reitera VEGA VEGA[659], quien, en la misma línea apuntada, afirma literalmente que:

> «Y es que, si tradicionalmente se ha venido identificando documento con todo escrito normalmente soportado en papel (otros soportes –papiro, pergamino, arcilla– han desaparecido en la práctica para la escritura), hoy en día ha cambiado la concepción de documento, y tanto la doctrina como la jurisprudencia han dejado de asimilar el soporte material del documento con el escrito[660] para extenderlo a nuevas realidades, tales como las cintas de vídeo o audio, películas fotográficas, discos digitales, magnéticos u ópticos, etc. De esta forma, surge un nuevo documento, el documento electrónico, que puede definirse como aquél que ha sido elaborado por medios electrónicos y que sólo puede ser leído con la ayuda de ciertos medios que hagan perceptibles las señales digitales».

---

Con anterioridad, incluso, al artículo 5.1 LMISI (norma que modifica este apartado 5 del artículo 3, según su Exposición de Motivos, para alinearlo en mayor medida con los conceptos utilizados en otras normas españolas de carácter general y en los países de nuestro entorno), el documento electrónico era definido como aquel «[…] redactado *en soporte electrónico* que incorpore datos *que estén firmados electrónicamente*» (la cursiva es propia), añadiendo, por tanto, al error de concepto anterior el derivado de la exclusión de todos aquellos documentos electrónicos que no se hallaran firmados (en la misma línea, RODRÍGUEZ HERNÁNDEZ, J., «Firma electrónica. Sus efectos jurídicos», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 6, 2004, p. 45).

[657] Entendiendo por *formato*, según la cuarta de las acepciones de la RAE, la «[e]structura de un disco dividido en campos y pistas según un determinado sistema operativo, lo que permite almacenar en él información».

[658] La cursiva es propia.

[659] VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., pp. 133 y 134; en la misma línea, DE ROSELLÓ MORENO, R., *El comercio electrónico y la protección de los consumidores*, cit., p. 38.

[660] En mi opinión, sin embargo, término mal empleado, pues, en lugar de la palabra *escrito*, hubiera sido más adecuado emplear la palabra *papel*. Y es que, como tuvimos ocasionar de argumentar, el registro escrito es una propiedad también compartida por aquellos documentos que no se encuentran en soporte físico papel, sino, como ahora, en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica.

Por lo demás, al igual que dijimos respecto de la firma electrónica, tampoco al documento electrónico podrá denegársele efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales «por el mero hecho de estar en formato electrónico[661]» (artículo 46 RIESCTE). Sin embargo, los problemas históricos existentes en torno a la noción de documento constituyeron, en su momento, la base doctrinal que condujo a la LECiv a reconocer jurídicamente aquello que son auténticos documentos electrónicos como medio de prueba (artículos 299.2 y 382 a 384), pero, bajo su denominación como *instrumentos*, a sacarlos fuera de la prueba documental (artículos 299.1.2.º y 3.º y 317 a 334)[662]. Así lo pone de manifiesto la propia norma cuando, en su Exposición de Motivos (apartado XI, párrafo 13º), afirma expresamente que:

> «[…] no habrá de forzarse la noción de prueba documental para incluir en ella lo que se aporte al proceso con fines de fijación de la certeza de los hechos, que no sea subsumible en las nociones de los restantes medios de prueba. Podrán confeccionarse y aportarse dictámenes e informes escritos, con sólo apariencia de documentos, pero de índole pericial o testifical y no es de excluir, sino que la ley lo prevé, la utilización de nuevos *instrumentos* probatorios, como soportes, hoy no convencionales, de datos, cifras y cuentas, a los que, en definitiva, haya de otorgárseles una consideración análoga a la de las pruebas documentales»[663].

En consecuencia, de la lectura de la LECiv cabe extraer cuatro conclusiones básicas: en primer lugar, a diferencia de otras ramas de nuestro ordenamiento jurídico, no se contiene definición legal alguna, a efectos procesales civiles, del término *documento*[664], cuestión que hubiera contribuido, indudablemente, a clarificar la cuestión que aquí se plantea; en segundo lugar, entiendo que no supone forzar la noción de prueba documental el hecho de concebir como documento algo que, por responder a su concepción clásica, también puede constar por escrito, si bien no está archivado en soporte físico papel, soporte físico que ahora se amplía (sin reemplazo alguno) a otros materiales aptos para el almacenamiento de contenido electrónico (cinta de vídeo o disco compacto, entre otros); en tercer lugar, tampoco fuerza

---

[661] Más apropiado que *formato electrónico*, en línea con la argumentación seguida, sería hablar de *soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica.*

[662] GOMES SOARES, F. S., «La prueba en la contratación electrónica de consumo», cit., p. 8; VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., p. 237.

[663] La cursiva es propia.

[664] RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, cit., p. 14.

la noción de prueba documental la inclusión en el término *documento* de aquellos otros contenidos que no constan archivados por escrito pero que, a través de la imagen o el sonido, pueden ser ya igualmente utilizados a efectos probatorios, y, en cuarto y último lugar, el error de concepto anterior obligó a situar lo que también debería ser prueba documental[665] (como es el documento electrónico, ya sea de naturaleza escrita, vista o hablada) en un apartado diferente, al que se le otorgó una eficacia probatoria también distinta, y menor: nos referimos al artículo 299.2 LECiv, que nos obliga a remitirnos, a su vez, a los artículos 382 a 384, concretamente al apartado tercero del primero de ellos, que establece una valoración de este medio de prueba conforme a las reglas de la sana crítica, muy distinta de la prueba plena de la que puede gozar (salvo que, en su caso, se impugne su autenticidad) la prueba documental al amparo de los artículos 299.1.2.º y 3.º y 317 a 334 LECiv[666].

---

[665] GONZÁLEZ GRANDA, P., «Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico», cit., pp. 27 y 28; ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, cit., pp. 35 y 36; VEGA VEGA, J. A., «El documento jurídico. Problemas de la electronificación», cit., p. 186.

[666] Criticando la opción legal escogida por la LECiv, *vid.* GOMES SOARES, F. S., «La prueba en la contratación electrónica de consumo», cit., p. 10, al entender que, con ello, «[…] sería posible penalizar con la prueba libre la utilización de los avances informáticos»; SANCHÍS CRESPO, C., *La prueba de soportes informáticos*, Valencia, Tirant lo Blanch, 1999, p. 141, quien sostiene que, cuando el objeto del reconocimiento es un soporte físico electrónico que representa hechos o actos con relevancia jurídica, la valoración libre supone desconocer la verdadera naturaleza de los mismos; SANCHÍS CRESPO, C./CHAVELI DONET, E. A., *La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000: doctrina, jurisprudencia y formularios*, Valencia, Tirant lo Blanch, 2002, p. 57, quienes, conjuntamente, afirman que «[l]a vigente LEC ha decidido mantener en el siglo XXI un concepto de documento que identifica como tales sólo a algunos de ellos, excluyendo deliberadamente a los documentos que han surgido de la mano de las nuevas tecnologías»; SERRA DOMÍNGUEZ, M., «La prueba documental», en ALONSO-CUEVILLAS SAYROL, J. (coord.) *Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000*, Madrid, Dijusa, 2000, p. 238, que, desde un punto de vista etimológico, hace referencia a la significación del documento como *dar a conocer*, de modo que, por tal, habrá de entenderse todo objeto que dé a conocer un hecho determinado. En contra de la postura anterior, pero partiendo, de nuevo, de una concepción errónea del término *escrito*, que lo asimila exclusivamente al soporte físico en papel, *vid.* ASENCIO MELLADO, J. M., *Derecho procesal civil*, Valencia, Tirant lo Blanch, 2015, p. 209, para quien, «[e]n efecto, y de una simple lectura de los textos legales que regulan este medio de prueba, especialmente de la Ley de Enjuiciamiento Civil y el Código Civil, se extrae la conclusión de que el documento no es otra cosa que una representación de la realidad plasmada por escrito. Documento susceptible de encuadrarse en el medio de prueba documental sólo sería el reflejado por medio de la escritura. Esta radical conclusión que bajo la vigencia de la anterior LEC suscitó graves inconvenientes dada la aparición en este siglo de medios a través de los cuales se representaba la realidad pero llevados a efectos en soportes de otra naturaleza (grabaciones videográficas, correo electrónico, etc.) se ha

En este contexto, y como consecuencia de la entrada en vigor de la LFE (D. A. 10ª), al artículo 326 LECiv se incorpora un apartado tercero que, a mayor abundamiento, entra en contradicción con el artículo 299.2 LECiv, al introducir una consideración a favor de la naturaleza electrónica del documento que no hace sino generar una suerte de confusión interpretativa en nada comprensible. En concreto, sostiene este nuevo apartado, «[c]uando la parte a quien interese la eficacia de un *documento electrónico* lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de firma electrónica»[667], aludiendo, ahora sí, al término *documento electrónico* e, indirectamente, a su naturaleza como prueba documental y desdiciendo todo cuanto, aún, consta en el texto de la LECiv respecto de la noción de *instrumento*, que no se modifica al objeto de imprimir una coherencia, si quiera mínima, respecto de la posible valoración de aquel como prueba documental. No se entiende, además, que introduzca el término únicamente en el apartado correspondiente a la fuerza probatoria de los documentos privados, si bien, como consecuencia de la remisión que en él hace al artículo 3 LFE, se estaría reconociendo implícitamente, no sólo el carácter de prueba documental de los documentos privados electrónicos, sino también el de los documentos públicos electrónicos (apartado 6 del artículo 3 LFE); todos ellos, por lo demás, tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable (apartado 7 del artículo 3 LFE), de modo que, por regla general, harán prueba plena en el proceso del hecho, acto o estado de cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que, en su caso, intervengan[668], salvo que su autenticidad sea impugnada por la parte a quien perjudique y de la impugnación se obtenga un resultado contrario a dicha autenticidad (artículos 319.1 y 326.1 LECiv).

La misma conclusión anterior cabrá extraer, como es lógico, cuando este documento electrónico conste de firma, también electrónica. Esta aclaración fue introducida originariamente

superado con nitidez y rotundidad al regularse un específico mecanismo para su incorporación diferenciada. La prueba documental, así, es la plasmada por la clásica escritura; los restantes medios que aparezcan en otro tipo de soportes se incorporarán a través de los mecanismos establecidos en los arts. 382 a 384».

667 La cursiva es propia.

668 A favor de esta postura, *vid.* ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 744.

por el artículo 3 LFE, cuyo apartado 8, *ab initio*, resolviendo la cuestión de la forma de incorporación al proceso, dispone que «[e]l soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio». Así, mientras que nada se dice claramente (aunque sí se entiende por deducción, como ya hemos apuntado) respecto del valor como prueba documental del documento electrónico en los apartados 5 a 7 del artículo 3 LFE, sí que se reconoce abiertamente este medio de prueba en relación con aquellos concretos documentos electrónicos dotados de firma electrónica (**anexo XXIII**). En cambio, no se indica nada respecto a qué sucedería en el supuesto de documentos en soporte papel dotados de firma electrónica, que (salvo que se traspasase la firma electrónica al soporte físico papel, codificándola de modo directamente legible –por ejemplo, empleando un código de barras–, con todas las dudas de validez y dificultades de aceptación que ello podría plantear), entendemos, tendrán un valor de prueba documental general, sin consideración alguna de la rúbrica, que, pese a estar plasmada, no podrá garantizar, en principio, las funciones de identificación autenticada, integridad, confidencialidad y/o no repudio.

De igual modo, por ser una modalidad específica de documento electrónico, también tendremos que entender que el contrato celebrado por vía electrónica gozará del mismo valor probatorio que aquel. Así lo pone de manifiesto, de hecho, el artículo 24 LSSICE[669], norma que surge en el intervalo que va desde la entrada en vigor de la LECiv hasta la promulgación de la LFE. Este artículo reconoce la admisibilidad como prueba documental del soporte electrónico en que conste un contrato celebrado por vía electrónica[670], cuya prueba se sujetará

[669] De acuerdo con la redacción dada por el artículo 4.10 LMISI.

[670] En concreto, dispone que «[e]n todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental». Más adecuado, entiendo, hubiera sido decir *el soporte físico distinto del papel apto para el archivo de información de naturaleza electrónica en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental*. En cualquier caso, como señala GONZÁLEZ GRANDA, P., «Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico», cit., p. 28, con esta medida, el legislador de la LSSICE pretende evitar los inconvenientes que la valoración libre podría acarrear en el ámbito negocial, incorporando el contrato electrónico a la prueba documental; en la misma línea se pronuncian MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., pp. 86 y 87, quienes también entienden que, en la práctica, el soporte físico en el que conste un contrato electrónico será, a estos efectos, una prueba documental y no una mera prueba complementaria sujeta a las reglas de la sana crítica. Ahora bien, indican con buen criterio GARCÍA MÁS, F. J. Y OTROS, «La contratación electrónica: modernidad y seguridad jurídica», cit., p. 129, debe quedar claro que lo que constituye la prueba documental no es el soporte en sí, sino puesto en relación con su contenido o con

a las reglas generales del ordenamiento jurídico (apartado segundo y párrafo primero del apartado primero). Así, en este concreto ámbito contractual electrónico, esta interpretación prevalecerá, sin duda alguna, sobre la inicial del artículo 299.2 LECiv, en virtud del principio general del Derecho de especialidad normativa (*lex specialis derogat legi generali*)[671] y del principio de temporalidad o cronología (*lex posterior derogat legi priori*), ambos considerados criterios tradicionales de solución de antinomias[672], entendidas estas como las contradicciones normativas que tienen lugar cuando, ante unas mismas situaciones fácticas, se imputan consecuencias

---

la información que suministra; en consecuencia, no debe confundirse el continente con el contenido, de modo que, lo mismo que le ocurre al soporte físico papel que está en blanco, el soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica, por sí solo, no tiene categoría de prueba documental.

[671] La formulación genérica del criterio de especialidad normativa como principio general del Derecho se encuentra de forma nítida en la STS de 16 de enero de 1998, F. J., 4º, y, de modo algo más confuso, en las SSTS de 25 de febrero de 1981, F. J. 2º; de 6 de octubre de 1986, F. J. 3º; de 27 de mayo de 1987, F. J. 2º; de 12 de diciembre de 1990, F. J. 7º; de 30 de abril de 1993, F. J. 3º; de 30 de octubre de 1993, F. J. 3º; de 29 de septiembre de 2000, F. J. 3º; de 28 de febrero de 2001, F. J. 5º, y de 20 de julio de 2005, F. J. 1º. Como en su momento señalara BOBBIO, N., *Teoria dell'ordinamento giuridico*, Turín, Giappichelli, 1957, pp. 100 y 344, el principio de especialidad normativa hace referencia a la materia regulada, al contenido de la norma, y supone el tránsito de una regla más amplia, que afecta a todo un género (en nuestro caso, la del documento, contenida en la LECiv), a una regla menos extensa, que afecta de manera exclusiva a una especie de dicho género (en nuestro caso, la del contrato electrónico, recogida en la LSSICE). Interesa destacar aquí que la norma que representa el género y la que regula la especie poseen elementos comunes, si bien la norma especial añade un dato ulterior a aquella que representa el género (IRTI, N., *La edad de la descodificación*, Vallirana, Bosch, 1992, p. 45). El principio de especialidad se ha desplegado de dos modos diferentes: como una cuestión de preferente aplicabilidad de una norma sobre otra o como un problema de vigencia de las mismas, es decir, de derogación de una norma por otra; VILLAR PALASÍ, J. L., *Derecho administrativo. Introducción y teoría de las normas*, Madrid, Universidad Complutense, 1968, pp. 483 y 484, sostiene que la regla de la especialidad presupone y no elimina la simultánea vigencia de la normas general y especial, aplicándose esta última cuando su supuesto de hecho se ajuste más adecuadamente al hecho concreto (pues, de otra manera, devendría ineficaz, ya que nunca sería aplicable) y aquella a todos los demás supuestos no encuadrables en la norma especial. A lo anterior debe añadirse que la norma general seguirá, incluso, siendo aplicable al supuesto regulado por la norma especial en todos aquellos aspectos no previstos por esta última (STS de 27 de octubre de 1979, F. J. 2º) y que la norma general no se aplicará supletoriamente a supuestos propios de una norma especial cuando se entienda que esta regula de modo suficiente los aspectos en cuestión (STC núm. 80/2002, de 8 de abril, F. J. 2º, y STS de 28 de febrero de 2001, F. J. 5º).

[672] TARDÍO PATO, J. A., «El principio de especialidad normativa (lex specialis) y sus aplicaciones jurisprudenciales», *Revista de Administración pública*, vol. 162, 2003, p. 189; sobre el origen y la evolución de estos

jurídicas que no pueden observarse simultáneamente[673]; en cualquier caso, difícilmente podrá negarse valor como prueba documental al documento electrónico que no adopte la forma de contrato electrónico, ya que, si a este último se le ha reconocido de modo explícito esta naturaleza, es precisamente por constituir una modalidad específica de aquella más general encarnada en el documento electrónico. Por lo demás, el artículo 24.1.2º LSSICE añadirá que, cuando estos contratos estén firmados electrónicamente, se estará a lo establecido en el artículo 3 LFE, haciendo una remisión indirecta al apartado octavo de este último precepto, cuyo inciso inicial, recordemos, reconoce el valor probatorio documental del documento (y, por ende, del contrato electrónico) acompañado de firma electrónica.

Al mismo tiempo, como bien es sabido, el ordenamiento jurídico comunitario se introduce en el Derecho español con todas sus normas, tanto de Derecho originario como de Derecho derivado, y es de aplicación prioritaria y directa sobre la norma interna que resulte incompatible, cualquiera que sea el rango que esta presente: la Constitución, los estatutos de autonomía, la legislación ordinaria y las disposiciones jurídicas de rango inferior, siempre que tengan el carácter de Derecho plenamente vigente en España[674]. En este sentido, la entrada

---

criterios, *vid.* VILLAR PALASÍ, J. L., «Más sobre las antinomias», en AA.VV. (coord.) *Don Luis Jordana de Pozas: creador de ciencia administrativa*, Madrid, Universidad Complutense, 2000, pp. 51 a 72.

673 PRIETO SANCHÍS, L., «Observaciones sobre las antinomias y el criterio de ponderación», *Cuadernos de Derecho público*, vol. 11, 2000, p. 10.

674 MARÍN LÓPEZ, A., «Orden jurídico internacional y Constitución española», *Revista de Derecho político*, vol. 45, 1999, pp. 48 y 49. Así lo reitera también, jurisdiccionalmente, el TC, y lo hace en numerosas ocasiones, destacando las siguientes: STC núm. 28/1991, de 14 de febrero, F. J. 4º, donde afirma que «[…] a partir de la fecha de su adhesión, el Reino de España se halla vinculado al Derecho de las Comunidades Europeas, originario y derivado, el cual –por decirlo con palabras del Tribunal de Justicia de las Comunidades Europeas– constituye un ordenamiento jurídico propio, integrado en el sistema jurídico de los Estados miembros y que se impone a sus órganos jurisdiccionales»; posteriormente, en su STC núm. 64/1991, de 22 de marzo, F. J. 1º, en la que el Tribunal sostiene, además, que «[…] los órganos judiciales no resolvieron los litigios planteados ante los mismos con arreglo al sistema de fuentes normativas consagrado por la Constitución, pues ignoraron el principio de primacía del Derecho comunitario europeo que rigen en nuestro ordenamiento desde el ingreso de España en la Comunidad Económica Europea», añadiendo, no obstante, en el mismo F. J., que «[…] la cesión del ejercicio de competencias en favor de organismos supranacionales no implica que las autoridades nacionales dejen de estar sometidas al ordenamiento interno cuando actúan cumpliendo obligaciones adquiridas frente a tales organismos, pues también en estos casos siguen siendo poder público que está sujeto a la Constitución y al resto del ordenamiento jurídico español (art. 9.1 CE)»; por último, la STC núm. 236/1991, de 12 de diciembre, F. J. 9º, en la que el Tribunal señala que «[…] la traslación de la normativa comunitaria derivada al derecho interno

en vigor del RIE-SCTE[675] –artículos 3.35) y 46– hubiera sido idónea para disipar todas las dudas que pudieran existir en torno al reconocimiento legal del documento electrónico en toda su extensión, aceptando su admisibilidad como prueba documental en todo procedimiento judicial, ya fuera como documento público electrónico (artículos 299.1.2º, 317 a 323 y 328 a 334 LECiv) o como documento privado electrónico (artículos 299.1.3º, 324 a 334 LECiv) y ya estuviera acompañado de firma electrónica o no lo estuviera. Sin embargo, como hemos visto, el artículo 46 Reglamento eIDAS tan sólo se limita a rechazar su posible denegación como prueba en juicio con base en su naturaleza electrónica, sin especificar si este valor probatorio será como prueba documental o como simple prueba sujeta a las reglas de la sana crítica. A esta confusión contribuye (en fase de tramitación parlamentaria, bien es cierto) el artículo 3.1.1º ALSEC, que, lejos de aclarar la cuestión en los extremos citados, se remite a la LECiv, limitándose a indicar que los documentos electrónicos tendrán la fuerza probatoria prevista en esta última Ley, sin incluir, ni siquiera, D. F. alguna que la modifique (tampoco al artículo 24.1.2º LSSICE) en el sentido de suprimir toda referencia hecha a la LFE a la que pretende derogar.

En definitiva, en la actualidad, y por lo que respecta a nuestro ordenamiento jurídico interno, nos encontramos con el siguiente panorama general, ordenado cronológicamente para una mejor comprensión:

1) Año 2000: la LECiv niega indirectamente la naturaleza documental (y, por ende, su carácter como prueba documental) de aquello que es un verdadero *documento*, el *documento electrónico*, evitando esta denominación y optando por la de *instrumento* (artículos 299.2 y 382 a 384 LECiv).

2) Año 2002: surge el artículo 24.2 LSSICE, que, reforzando nuestra teoría, reconoce por primera vez la naturaleza de prueba documental del contrato celebrado por vía electrónica, que entenderemos ampliada, no obstante, a la categoría más general de documento electrónico por ser esta la que a aquel engloba e integra. Más tarde, añadirá un párrafo

ha de seguir necesariamente los criterios constitucionales y estatutarios de reparto de competencias entre el Estado y las Comunidades Autónomas, criterios que, de no procederse a su revisión por los cauces correspondientes (art. 95.1 de la Constitución), no resultan alterados ni por el ingreso de España en la CEE ni por la promulgación de normas comunitarias». En la misma línea, las SSTC núm. 79/1992, de 28 de mayo, F. J. 1º; núm. 172/1992, de 29 de octubre, F. J. 1º; núm. 180/1993, de 31 de mayo, F. J. 3º.

[675] Nada decía al respecto la derogada DFE.

segundo al apartado primero que dispone que cuando estos contratos estén firmados electrónicamente se estará a lo establecido en el artículo 3 LFE, más específicamente al artículo 3.8 LFE, cuyo inciso inicial reconoce el valor de prueba documental en juicio del documento acompañado de firma electrónica.

3) Año 2003 (1): nace la LFE, cuyo artículo 3, apartados 5 a 7, define por primera vez en nuestro país el documento electrónico y reconoce su posible naturaleza como documento público y como documento privado, que tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, no reconociéndose abiertamente el valor de esta figura como prueba documental; sí lo hará, en cambio, del documento firmado electrónicamente.

4) Año 2003 (2): como consecuencia de la entrada en vigor de esta última Ley, y sin modificar su postura inicial, la LECiv introduce en su artículo 326 un apartado tercero en el que, ahora sí, habla expresamente de documento electrónico, remitiéndose al artículo 3 LFE para aquellos casos en que la parte a quien interese su eficacia lo pida o se impugne su autenticidad. Y lo hace en el apartado correspondiente a la fuerza probatoria de los documentos privados, sin parecer advertir que, en ese mismo artículo 3 LFE, se reconoce también la posible naturaleza pública del documento electrónico (artículo 3.5.2º y 6), que no encontrará en la LECiv respuesta alguna para el caso en que la parte a quien interese su eficacia también lo pida o se impugne su autenticidad.

5) Año 2014: aparece el RIE-SCTE, que incorpora por primera al ordenamiento jurídico comunitario la noción de documento electrónico, de manera tanto más adecuada a como lo hiciera la LFE, prohibiendo que puedan denegarse efectos jurídicos y admisibilidad como prueba en procedimientos judiciales a un documento electrónico por el mero hecho de estar en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica. Sin embargo, nada dice respecto de su posible valor como prueba documental.

6) Año por determinar, pero posterior a 2014: tras la entrada en vigor del Reglamento eIDAS, es elaborado el ALSEC (que prevé la derogación de la LFE), cuyo artículo 3.1.1º reconoce la existencia del documento electrónico, pero, incomprensiblemente por la tendencia marcada por la LSSICE y por la LFE, no se pronuncia respecto de la eficacia procesal del mismo, remitiéndose, en su lugar, a la LECiv y, con ello, a los problemas de incongruencia apuntados, que, en ningún momento, pretenden ser subsanados por el

nuevo Anteproyecto. Además, el texto no se verá acompañado de ninguna D. F. que suprima las referencias hechas a la LFE, tanto en la LECiv como en la LSSICE, pese a pretender su íntegra derogación.

Consecuencia de esta última remisión a la LECiv, y dada la concisión del contenido del artículo 3.1.1º ALSEC, de promulgarse finalmente el texto en los términos expuestos, volveríamos a una situación en la que, si bien se reconoce ya abiertamente la existencia de la figura del documento electrónico, nada claro hay, al menos explícitamente, respecto de su valor como prueba documental. Ahora bien, al emplearse esta noción (*documento electrónico*), implícitamente se estaría reconociendo su eficacia procesal general como prueba documental (también, por ende, la del contrato electrónico, algo que ya venía reconocido por la LSSICE), pero no hubiera venido mal (más bien lo contrario) que, a efectos de seguridad jurídica, se hubiera suprimido toda referencia a la noción de *instrumento* por parte del artículo 299.2 LECiv y se hubiera reconocido, paralelamente, la explícita naturaleza y la admisibilidad como prueba documental en juicio del, ya sí, documento electrónico, ya sea como documento público electrónico (artículos 299.1.2º, 317 a 323 y 328 a 334 LECiv) o como documento privado electrónico (artículos 299.1.3º, 324 a 334 LECiv), con firma electrónica o sin ella.

### 2.2. Solicitud de eficacia o impugnación de un contrato acompañado de firma electrónica

Una vez expuesto el estado de la cuestión respecto de los efectos jurídicos de la firma electrónica, primero, y del controvertido valor probatorio general del contrato electrónico como documento electrónico que es (público o privado, con o sin firma electrónica), después, el siguiente paso, aunando ambas figuras, llevaría a analizar qué sucede cuando determinadas propiedades presumiblemente inherentes a contratos de esta naturaleza son impugnadas en juicio o cuando la parte a quien interese su eficacia así lo pida. El Reglamento eIDAS no responde a esta cuestión, que quedaría regulada a nivel interno, si finalmente se promulga el texto, por el artículo 3.1. 2º a 4º ALSEC.

Como pusimos de manifiesto, este Anteproyecto no lleva aparejada, como debería, la modificación de la referencia que el artículo 326.3 LECiv (además del artículo 24.1.2º LSSICE) hace al artículo 3 LFE, cuya derogación prevé el ALSEC. De haberse previsto la misma, el precepto de la LECiv podría haber quedado como sigue: *cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, integridad, precisión de fecha y hora u otras características de un documento electrónico, se procederá con arreglo a lo establecido en el artículo 3 de la Ley*

*reguladora de determinados aspectos de los servicios electrónicos de confianza*, reconfigurando, así, el puente habilitador necesario ya previsto por el artículo 3.1.1º ALSEC.

Realizada esta modificación, habríamos de acudir, en primer lugar, al artículo 3.1.2º ALSEC, que, con una redacción prácticamente idéntica, se limita a establecer que «[c]uando la autenticidad, integridad, precisión de fecha y hora u otras características de un documento electrónico se pongan en duda o la parte a quien interese su eficacia lo pida, se practicará prueba para acreditar dichos extremos». De darse el supuesto previsto en dicho apartado, procedería determinar la actuación desde un punto de vista procesal ante dos situaciones posibles: una primera, representada por aquellos casos en que el contrato celebrado por vía electrónica no disponga (al no ser necesario, como regla general, para su validez y eficacia) de firma electrónica; una segunda, por aquellos otros en que el contrato electrónico sí conste de rúbrica, también electrónica (**anexo XXIV**).

En el primero de los supuestos, aclaradas todas las dudas en torno a la existencia misma del documento electrónico –artículos 3.35) y 46 RIE-SCTE, 3 LFE y 3 ALSEC–, de una parte, y al reconocimiento del mismo como medio de prueba documental (por deducción, aunque también en modo explícito, para el contrato electrónico por el artículo 24.2 LSSICE), de otra, sería necesario determinar si estamos en presencia de un contrato electrónico de naturaleza pública[676] (cuyo análisis escapa de nuestro objeto de estudio) o de naturaleza privada. Ninguna definición aporta el Reglamento eIDAS ni el correspondiente Anteproyecto de este extremo, habiendo de acudir, hasta el momento en que se produzca su derogación, al artículo 3.6 LFE, único precepto que describe en qué casos estaremos en presencia de un documento electrónico público o de un documento electrónico privado:

[676] Como bien indican para el supuesto del contrato electrónico (y, por extensión, para el del documento electrónico) MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., pp. 84 y 85, «[n]o es límite a lo anterior el hecho de que en algún supuesto resulte exigida la elevación a documento público de un determinado contrato o su inscripción en un registro público (lo que de ordinario requiere el previo otorgamiento de escritura pública). Cuando tal sea el caso, dispone el art. 23.4 LSSICE, esa exigencia habrá de regirse por la legislación específica que la impone. No significa esto, como es natural, que estas materias queden vedadas a la contratación electrónica, sino que en tal caso habrá de estarse a lo que disponga la norma especialmente aplicable».

> «El documento electrónico será soporte de: a) documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso; b) documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica, y c) documentos privados».

Sin embargo, este apartado incurre en una contradicción manifiesta con la nueva noción de documento electrónico resultante de la modificación experimentada por la LMISI. En efecto, mientras que el modificado artículo 3.5 LFE elimina la necesidad de que el documento electrónico tenga que estar firmado electrónicamente, en una previsión adecuada al objeto de ampliar la regulación también a aquellos documentos electrónicos que no consten de rúbrica, los apartados a) y b) del artículo 3.6 LFE, a la hora de regular el soporte público en que dicho documento puede constar, exige que este venga firmado (aun sin especificar tampoco la modalidad de firma electrónica –simple, avanzada o reconocida– necesaria a estos efectos), excluyendo, por tanto, todos los demás supuestos en que el documento público electrónicos no conste de firma electrónica[677]. Por lo demás, de derogarse la LFE y no modificarse la redacción del artículo 3 ALSEC incorporando este extremo, tendríamos que aplicar por analogía los artículos 317 y 324 LECiv para poder llegar a la misma solución.

Aclarada esta cuestión, acudiríamos a continuación al apartado séptimo del artículo 3 LFE, que sostiene que los documentos electrónicos tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable. En lo que aquí interesa, habríamos de analizar su fuerza probatoria, regulada en el artículo 319, para los documentos electrónicos públicos, y en el artículo 326, para los documentos electrónicos privados, ambos de la LECiv. En relación a estos últimos, dispone el artículo 326.2 LECiv, «[c]uando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto». Adaptado al ámbito electrónico, este cotejo pericial de letras carece de utilidad al desparecer la forma manuscrita, de modo que únicamente podríamos acudir a la previsión final, redactada a modo de cajón de sastre en el que incluir cualquier medio de prueba que permita determinar la autenticidad, la integridad,

[677] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 88.

la precisión de fecha y hora o cualquier otra característica del documento electrónico; especialmente útil sería, al respecto, la prueba pericial informática. En cualquier caso, si del medio de prueba que, en su caso, se emplee se obtiene un resultado positivo, se procederá conforme a lo previsto en el apartado tercero del artículo 320 LECiv, de modo que las costas, gastos y derechos originados serán exclusivamente de cargo de quien hubiese formulado la impugnación, pudiendo imponérsele, además, una multa de entre 120 a 600 euros en el caso de que aquella hubiese sido temeraria; caso de no poderse deducir la autenticidad, la integridad, la precisión de fecha y hora o cualquier otra característica del documento electrónico, o de no proponerse prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

Nada dice el artículo 326.2 LECiv en relación con aquellos supuestos en que haya de determinarse la fuerza probatoria del documento electrónico, no porque haya sido impugnado, sino porque la parte a quien interese su eficacia así lo pida; no obstante, entendemos que debería procederse de idéntica manera, salvo en lo que tenga que ver con el sujeto que haya de asumir las costas, gastos y derechos originados, que pasarán a ser exclusivamente de cargo de quien hubiese formulado la solicitud de eficacia, no procediendo en estos casos, entiendo, multa alguna por temeridad. Justo sobre esta cuestión viene a pronunciarse el artículo 3.1.4º ALSEC, que, al contrario de lo que acabamos de indicar, sólo regula el supuesto en que la eficacia del documento sea solicitada por la parte a quien interese, y lo hace estableciendo, en línea con cuanto acabamos de indicar, que la parte a quien beneficie el documento deberá correr con los gastos del informe pericial que se solicite, no indicando nada para los supuestos de impugnación, que seguirían rigiéndose por lo dispuesto en la LECiv.

En el segundo supuesto, tampoco existen dudas respecto de su valor, a efectos procesales, como medio de prueba documental, pues así lo afirma expresamente el artículo 3.8, *ab initio*, LFE, precepto al que, para el caso de los contratos electrónicos, se remite el artículo 24.1.2º LSSICE. De derogarse el primero y, por lógica, la redacción afectada de este segundo, nada impediría seguir manteniendo esta concepción probatoria del contrato electrónico si tenemos en cuenta el hecho, tantas veces reiterado, de su pertenencia a la categoría más amplia integrada por el documento electrónico; en cualquier caso, nada dice al respecto ni el RIE-SCTE ni el ALSEC. Por lo demás, de la misma manera que en el supuesto anterior habría que proceder a la hora de determinar, en primer lugar, la naturaleza, pública o privada, del contrato firmado electrónicamente y, tras ello, en segundo lugar, el proceso de solicitud de eficacia o de impugnación de la autenticidad, la integridad, la precisión de fecha y hora o cualquier otra característica del contrato electrónico privado.

Sin embargo, si el aspecto que concretamente se impugna[678] dentro del contrato electrónico (al que, en este supuesto, se incluiría el contrato tradicional por la interpretación extensiva posibilitada por la entrada en vigor del actual artículo 3.8, *ab initio*, LFE) es la autenticidad de la rúbrica con que la se hallan firmados electrónicamente los datos incorporados a esta modalidad de documento, será preciso acudir, hasta tanto sea derogado (habida cuenta de que en nada contradice el contenido del RIE-SCTE), al artículo 3.8 LFE[679]. Este precepto realiza una clara separación entre firma electrónica reconocida y firma electrónica avanzada; nada dice de la firma electrónica simple, que, a efectos de comprobación de la autenticidad, quedaría subsumida, entiendo, en el procedimiento descrito para este segundo tipo o modalidad de firma[680]. Del resultado de la comprobación que a continuación se describe dependerá

[678] No cabe aquí, entiendo, solicitar su eficacia, que sólo podrá hacerse del texto en el que la firma electrónica se inserte.

[679] Este apartado fue objeto de modificación por el artículo 5.2 LMISI, con el objetivo de «[…] clarificar las reglas de valoración de la firma electrónica en juicio». Hasta ese momento y en lo que aquí interesa, la redacción que presentaba era la siguiente: «[…] si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumplen todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la confidencialidad del proceso así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes. Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil». Por tanto, la redacción inicial del artículo 3.8 LFE establecía que se procedería a comprobar el cumplimiento, por parte del PSSIc, de los requisitos legales que, precisamente, pretenden proporcionar seguridad a la firma electrónica y cuyo incumplimiento podría generar dudas sobre la fiabilidad de la misma. Empero, existen también otros elementos y circunstancias que pueden influir igualmente a la hora de determinar la fiabilidad de la firma electrónica y que no están relacionados con el PSSIc (ya PSSIisc), no estando previstos, en ese momento, en dicho precepto (a no ser que la enumeración legal fuera simplemente ejemplificativa y no *numerus clausus* o que, además de esta previsión, se considerara también aplicable la prevista respecto de la impugnación de la firma electrónica avanzada): es el caso de la falta de fiabilidad por escasa calidad de las claves de firma electrónica (que no necesariamente son generadas por el PSSIc) o por falta de seguridad del dispositivo de creación de firma electrónica empleado (que no ha de ser necesariamente adquirido al PSSIc).

[680] Así lo entienden también ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 46, quienes afirman que «[…] no puede entenderse que el olvido del legislador conlleve que no hay prueba a realizar en caso de impugnación de una firma electrónica ordinaria, que

la autenticidad (o no) de la firma electrónica en cuestión (mejor dicho, como veremos, la validez y eficacia de la firma electrónica, a la que habría de añadirse necesariamente la autenticidad de la misma) y, por ende, la identificación autenticada (o no), la integridad (o no), la confidencialidad (o no) y/o el no repudio (o no) del contrato electrónico en el que esté incorporada, por ser estas las características específicas que este SSIisc (dependiendo de la modalidad de firma electrónica por la que se opte y de la seguridad que imprima) puede llegar a garantizar (**anexo XXV**).

De acuerdo con el artículo 3.8.1º y 2º LFE, si lo que se impugna es la autenticidad de la firma electrónica reconocida, se procederá a comprobar que esta cumple tres extremos concretos que determinan su validez y existencia como tal: en primer lugar, que se trata de una firma electrónica avanzada basada en un certificado electrónico reconocido; en segundo lugar, que cumple todos los requisitos y condiciones establecidos en la LFE para este tipo de certificados, y, en tercer y último lugar, que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica (artículo 3.8.1º LFE). Ahora bien, podría darse el caso, ya apuntado por la doctrina[681], de que, por darse los requisitos anteriores, una firma electrónica reconocida fuera válida y eficaz, pero no fuera auténtica, que es lo que verdaderamente se está impugnando (es esto lo que sucedería cuando, por ejemplo, se produce una incorrecta identificación del solicitante del certificado o se pierden las claves privadas de firma electrónica, realizándose la misma por un tercero no autorizado); *sensu contrario*, cabría la posibilidad de que la firma electrónica reconocida no fuera valida y eficaz por no darse cumulativamente los requisitos exigidos por el artículo 3.8.1º y, sin embargo, sí fuera auténtica (por ejemplo, por no haberse producido la comprobación presencial de la identidad del solicitante del certificado pero, pese a ello, ser correctamente identificado). Por ende, entiendo que, en todos estos casos, se deberá probar que la firma electrónica reconocida es válida, eficaz y auténtica, de modo tal que el proceso nunca pueda concluir válidamente con la sola concurrencia aislada de alguno de estos elementos.

Por lo demás, la carga de realizar tales comprobaciones, o, lo que es lo mismo, la carga de la prueba, recaerá en aquel que haya presentado a prueba el contrato electrónico cuya firma electrónica es objeto de impugnación. Si el resultado de las comprobaciones es positivo en

---

por cierto es la que más impugnaciones potenciales puede tener, dado que es la menos fiable»; en la misma línea, FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 56.

[681] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 97.

los términos indicados en el párrafo anterior, se habrá de presumir la validez, eficacia y autenticidad de la firma electrónica reconocida comprobada e, indirectamente, en principio, la identificación autenticada del emisor, la integridad y el no repudio en origen del contrato electrónico aportado al proceso, siempre que este no requiera de ulteriores comprobaciones adicionales que puedan comprometer el cumplimiento de estas propiedades. En este caso, las costas, gastos y derechos que origine la comprobación serán exclusivamente a cargo de quien hubiese formulado la impugnación, pudiéndosele imponer, además, una multa de 120 a 600 euros si, a juicio del tribunal, aquella hubiese sido temeraria (artículo 3.8.2º LFE). Se echa en falta, sin embargo, una previsión similar a la que, por remisión al artículo 326.2 LFE, sí que se contempla respecto de la impugnación de la autenticidad de una firma electrónica avanzada, en la que se establece que, si de la prueba practicada no puede deducirse la autenticidad o si no se hubiese propuesto prueba alguna, el tribunal la valorará conforme a las reglas de la sana crítica[682]; ello permitirá la libre valoración por el juez de una firma electrónica respecto de la que, si bien no se ha podido probar su carácter de reconocida, sí que, pese a ello, puede garantizar la autoría, integridad, autenticidad y/o no repudio del documento electrónico afectado.

En cambio, si la impugnación afecta a una firma electrónica avanzada, se procederá conforme indica el artículo 326.2 LECiv, ya analizado a la hora de analizar el proceso a seguir en el supuesto en que se impugne la autenticidad de un documento privado y al que, por ende, nos remitimos[683]. Lo mismo sucederá, entendíamos, si estamos en presencia de una firma electrónica simple, pese a que nada dice la LFE.

De derogarse finalmente la LFE, tendríamos que acudir a la norma encargada de regular determinados aspectos de los servicios electrónicos de confianza en nuestro ordenamiento jurídico interno como complemento del RIE-SCTE. Esta norma parece venir representada en la actualidad por el ALSEC, cuyo artículo 3.1.3º tan sólo se limita a establecer que si se hubiera utilizado en estos casos una firma electrónica cualificada, se presumirá: de una parte,

---

[682] *Ibid.*, p. 98.

[683] No se establece aquí criterio alguna de prueba, dado que, en aplicación del principio de neutralidad tecnológica, cualquier tecnología puede ser empleada para la firma electrónica avanzada (también para la simple), haga uso o no de certificados electrónicos o de dispositivos de firma electrónica (ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., pp. 746 y 747).

que el documento electrónico reúne las características cuestionadas; de otra, que la firma electrónica se ha prestado correctamente si figuraba, «[…] en el momento relevante a los efectos de la discrepancia», en la lista de PSSIisc y SSIisc cualificados regulada en los artículos 22 RIE-SCTE y 19 ALSEC. Si, aun así, se requiriera un informe pericial *ad hoc*, los gastos serán de cuenta de la parte que solicitó este informe. En este caso, parece ser que lo que hace el artículo 3.1.3º del Anteproyecto es determinar el efecto que supondría contar con una firma electrónica cualificada en un documento electrónico impugnado o cuya eficacia se solicita, sin aclarar si a este efecto se llega por impugnación previa, o no, de la autenticidad de dicha firma electrónica cualificada y sin indicar qué sucedería si la firma electrónica fuera simple o avanzada.

Así, por tanto, mientras que la LFE regula de manera directa la posible impugnación de la autenticidad de una firma electrónica, estableciendo las consecuencias que tendría el resultado, positivo o negativo, obtenido (y que, como indicábamos, afectará consecuente pero indirectamente, en principio, a la identificación autenticada del emisor, a la integridad y al no repudio en origen del documento electrónico en que la firma electrónica se inserte), el ALSEC disciplina los efectos que la firma electrónica cualificada tendría en caso de impugnación de la autenticidad, integridad, precisión de fecha y hora u otras características del documento electrónico con ella firmado. La ventaja del primer caso es que, una vez sepamos si la firma electrónica impugnada es auténtica, válida y eficaz, por simple deducción podremos determinar también aquello que garantizará del documento electrónico al que se vincula, además de saber el procedimiento a seguir en el caso de que se impugne una firma electrónica avanzada y, entiendo, simple; la ventaja del segundo supuesto, en cambio, es que indica, ahora sí de manera directa, las propiedades que tendrá el documento electrónico cuando conste de firma electrónica cualificada, pero nada dice, ni directa ni indirectamente, acerca de si ese efecto previsto para la firma electrónica cualificada (presumir que el documento electrónico reúne las características impugnadas) se produciría también en el caso de que, previamente, se hubiese impugnado la autenticidad de la misma o qué efectos tendría la firma electrónica simple o avanzada. Es por ello que lo más adecuado, en mi opinión, sería subsanar los defectos que ambas presentan y modificar y actualizar[684] los apartados correspondientes (y consecutivos al actual artículo 3.1.1º ALSEC) del precepto del Anteproyecto que haya de entrar

[684] La actualización vendría determinada, fundamentalmente, por la sustitución de los términos *firma electrónica reconocida* por *firma electrónica cualificada*, *certificado reconocido de firma electrónica* por *certificado cualificado de firma electrónica* y *dispositivo seguro de creación de firma electrónica* por *dispositivo cualificado de creación de firma electrónica*.

en vigor tras la derogación de la LFE, pudiendo quedar como sigue[685]: […] *2. El documento electrónico en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Ccuando la autenticidad, integridad, precisión de fecha y hora u otras características de un documento electrónico se pongan en duda o la parte a quien interese su eficacia lo pida, se practicará prueba para acreditar dichos extremos. 3. Si lo que se impugnare fuera la autenticidad de la firma electrónica cualificada con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado cualificado de firma electrónica, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo cualificado de creación de firma electrónica. La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica cualificada. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la validez, eficacia y autenticidad de la firma electrónica cualificada y la identificación autenticada del emisor, la integridad y el no repudio en origen del documento electrónico firmado electrónicamente, siendo las costas, gastos y derechos que origine la comprobación exclusivamente a cargo de quien hubiese formulado la impugnación; si, a juicio del tribunal, la impugnación hubiese sido temeraria, podrá imponerle, además, una multa de 120 a 600 euros. Si de la prueba practicada no puede deducirse la autenticidad o si no se hubiese propuesto prueba alguna, el tribunal la valorará conforme a las reglas de la sana crítica. También se presumirá que la firma electrónica se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de confianza del artículo 22 del Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio; si, aun así, se requiriera un informe pericial "ad hoc", los gastos serán de cuenta de la parte que solicitó este informe. 4. Si se impugna la autenticidad de la firma electrónica simple o de la firma electrónica avanzada con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil.*

### 2.3. Aportación al proceso de contratos electrónicos de naturaleza privada

Admitida la naturaleza de prueba documental del documento electrónico privado en su modalidad contractual, cabría preguntarse también por el procedimiento en virtud del cual puede ser este aportado al proceso. Dada la ausencia de toda norma específica en la legislación sobre de firma electrónica, habrá de estarse a las reglas generales sobre la materia; en concreto, al artículo 265.1.1º LECiv, en virtud del cual «[a] toda demanda o contestación

[685] No se contiene, en este supuesto, una regulación de todos los servicios de confianza, como sí hace la ALSEC. La finalidad es dejar clara la comparativa con la norma precedente, especialmente útil a los efectos del presente estudio.

habrán de acompañarse: los documentos en que las partes funden su derecho a la tutela judicial que pretenden». No obstante, prosigue el apartado segundo del precepto estableciendo una excepción a lo anterior:

> «Sólo cuando las partes, al presentar su demanda o contestación, no puedan disponer de los documentos, medios e instrumentos a que se refieren los tres primeros números del apartado anterior, podrán designar el archivo, protocolo o lugar en que se encuentren, o el registro, libro registro, actuaciones o expediente del que se pretenda obtener una certificación.
>
> Si lo que pretenda aportarse al proceso se encontrara en archivo, protocolo, expediente o registro del que se puedan pedir y obtener copias fehacientes, se entenderá que el actor dispone de ello y deberá acompañarlo a la demanda, sin que pueda limitarse a efectuar la designación a que se refiere el párrafo anterior».

En cuanto a la forma en que habrán de presentarse, el artículo 325 LECiv nos remite, a su vez, al previo artículo 268.1 de esta misma Ley, que dispone que:

> «1. Los documentos privados que hayan de aportarse se presentarán en original o mediante copia autenticada por el fedatario público competente y se unirán a los autos o se dejará testimonio de ellos, con devolución de los originales o copias fehacientes presentadas, si así lo solicitan los interesados. Estos documentos podrán ser también presentados mediante imágenes digitalizadas, incorporadas a anexos firmados electrónicamente.
>
> 2. Si la parte sólo posee copia simple del documento privado, podrá presentar ésta, ya sea en soporte papel o mediante imagen digitalizada en la forma descrita en el apartado anterior, que surtirá los mismos efectos que el original, siempre que la conformidad de aquélla con éste no sea cuestionada por cualquiera de las demás partes.
>
> 3. En el caso de que el original del documento privado se encuentre en un expediente, protocolo, archivo o registro público, se presentará copia auténtica o se designará el archivo, protocolo o registro, según lo dispuesto en el apartado 2 del artículo 265».

Obviamente, se está refiriendo a los documentos privados en soporte físico papel, que, a los que efectos que aquí nos interesan, entendemos que podrían presentarse, no sólo con

firma manuscrita, sino también con firma electrónica codificada de modo directamente legible, si bien esta opción tendría que pactarse previamente entre las partes, presentando el inconveniente de la posterior aceptación por el Juez y la contraparte[686].

En cuanto a los documentos privados en soporte físico distinto del papel pero apto para el archivo de información de naturaleza electrónica dotados, o no, de firma electrónica, la solución adecuada pasa por la creación de un procedimiento de aportación de los mismos, realizado por la representación procesal de la parte a quien interese su aportación. Esta opción encuentra cobijo en el artículo 135 LECiv, estableciendo lo siguiente:

> «1. Cuando las oficinas judiciales y los sujetos intervinientes en un proceso estén obligados al empleo de los sistemas telemáticos o electrónicos existentes en la Administración de Justicia conforme al artículo 273, remitirán y recibirán todos los escritos, iniciadores o no, y demás documentos a través de estos sistemas, salvo las excepciones establecidas en la ley, de forma tal que esté garantizada la autenticidad de la comunicación y quede constancia fehaciente de la remisión y la recepción íntegras, así como de la fecha en que éstas se hicieren. Esto será también de aplicación a aquellos intervinientes que, sin estar obligados, opten por el uso de los sistemas telemáticos o electrónicos.
>
> Se podrán presentar escritos y documentos en formato electrónico todos los días del año durante las veinticuatro horas.
>
> Presentados los escritos y documentos por medios telemáticos, se emitirá automáticamente recibo por el mismo medio, con expresión del número de entrada de registro y de la fecha y la hora de presentación, en la que se tendrán por presentados a todos los efectos. En caso de que la presentación tenga lugar en día u hora inhábil a efectos procesales conforme a la ley, se entenderá efectuada el primer día y hora hábil siguiente.
>
> A efectos de prueba y del cumplimiento de requisitos legales que exijan disponer de los documentos originales o de copias fehacientes, se estará a lo previsto en el artículo 162.
>
> 2. Cuando la presentación de escritos perentorios dentro de plazo por los medios telemáticos o electrónicos a que se refiere el apartado anterior no sea posible por interrupción no planificada del servicio de comunicaciones telemáticas o electrónicas, siempre que sea posible se dispondrán las medidas para que el usuario resulte informado de esta circunstancia, así como de los efectos

[686] ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., pp. 40 y 41.

de la suspensión, con indicación expresa, en su caso, de la prórroga de los plazos de inminente vencimiento. El remitente podrá proceder, en este caso, a su presentación en la oficina judicial el primer día hábil siguiente acompañando el justificante de dicha interrupción.

En los casos de interrupción planificada deberá anunciarse con la antelación suficiente, informando de los medios alternativos de presentación que en tal caso procedan.

3. Si el servicio de comunicaciones telemáticas o electrónicas resultase insuficiente para la presentación de los escritos o documentos, se deberá presentar en soporte electrónico en la oficina judicial ese día o el día siguiente hábil, junto con el justificante expedido por el servidor de haber intentado la presentación sin éxito. En estos casos, se entregará recibo de su recepción.

4. Sin perjuicio de lo anterior, los escritos y documentos se presentarán en soporte papel cuando los interesados no estén obligados a utilizar los medios telemáticos y no hubieran optado por ello, cuando no sean susceptibles de conversión en formato electrónico y en los demás supuestos previstos en las leyes. Estos documentos, así como los instrumentos o efectos que se acompañen quedarán depositados y custodiados en el archivo, de gestión o definitivo, de la oficina judicial, a disposición de las partes, asignándoseles un número de orden, y dejando constancia en el expediente judicial electrónico de su existencia.

En caso de presentación de escritos y documentos en soporte papel, el funcionario designado para ello estampará en los escritos de iniciación del procedimiento y de cualesquiera otros cuya presentación esté sujeta a plazo perentorio el correspondiente sello en el que se hará constar la oficina judicial ante la que se presenta y el día y hora de la presentación.

5. La presentación de escritos y documentos, cualquiera que fuera la forma, si estuviere sujeta a plazo, podrá efectuarse hasta las quince horas del día hábil siguiente al del vencimiento del plazo.

En las actuaciones ante los tribunales civiles, no se admitirá la presentación de escritos en el juzgado que preste el servicio de guardia».

Finalmente, en lo que atañe a la documentación de las actuaciones, el artículo 146.3 LECiv establece que los tribunales tendrán la posibilidad de emplear medios técnicos de documentación y archivo, tanto de sus actuaciones como de los escritos y documentos que reciban;

todo ello con las garantías del *supra* expuesto artículo 135.1 LECiv. Asimismo, podrán emplear medios técnicos de seguimiento del estado de los distintos procesos y de estadística relativa a estos[687].

[687] Para un estudio más profundo de esta cuestión, *vid.* ELÍAS BATURONES, J. J., *La prueba de documentos electrónicos en los tribunales de justicia*, cit., pp. 39 a 53.

# CAPÍTULO CUARTO
# ELEMENTOS SUBJETIVOS DEL SISTEMA DE FIRMA ELECTRÓNICA

**SUMARIO**. - **I.** IDENTIFICACIÓN Y AUTENTICACIÓN ELECTRÓNICAS. **1.** Reconocimiento transfronterizo de los medios de identificación electrónica. **2.** El Documento Nacional de Identidad electrónico como medio de identificación electrónica preeminente en la normativa española tradicional. **II.** ESTRUCTURA TRIANGULAR DEL SISTEMA DE FIRMA ELECTRÓNICA. **1.** Firmante. **2.** Tercero que confía. **3.** Tercero generador de confianza como sujeto activo intermediador: el problema de la descoordinación normativa. **3.1.** Ámbito de aplicación y principios rectores de la actividad. **3.1.1.** Principio de aplicación de la ley del país de origen. **3.1.2.** Principio de reconocimiento mutuo o de libre prestación de servicios de la sociedad de la información. **3.1.3.** Principio de no sujeción a autorización previa. **3.2.** Obligaciones. **3.2.1.** Generales o comunes a todos los prestadores de servicios de la sociedad de la información. **3.2.2.** Específicas o concretas de los prestadores de servicios de intermediación. **3.2.3.** Propias o singulares de los prestadores de servicios de confianza. **3.3.** Régimen de responsabilidad. **3.4.** Régimen de supervisión y control. **3.5.** Régimen de infracciones y sanciones. **3.5.1.** Afectados. **3.5.2.** Supuestos. **3.5.3.** Imposición.

## I. IDENTIFICACIÓN Y AUTENTICACIÓN ELECTRÓNICAS

La identificación electrónica ha sido objeto de tratamiento jurídico en multitud de instrumentos anteriores a la promulgación del RIE-SCTE, principalmente sustentados en la legislación en materia de administración electrónica (también, en menor medida, en las normas sobre protección de datos de carácter personal), con la única excepción del DNIe, de carácter autónomo[688]. En efecto, al igual que sucede con la autenticación, la identificación aparece

[688] ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 679.

mencionada en muy diversas normas jurídicas de distinta naturaleza, con frecuencia a los fines de imponerla como requisito necesario para la realización de una actuación, ya sea del ciudadano o de la propia Administración, posibilitándose el uso de diversos medios técnicos para tales fines[689].

Menos frecuente será, sin embargo, encontrar una definición legal general de identificación electrónica, habiendo de acudir, por su relevancia, a la proporcionada precisamente por el nuevo Reglamento europeo eIDAS. De acuerdo con este Reglamento, la *identificación electrónica* (artículos 6 a 12) hace alusión al «[…] proceso de utilizar los datos de identificación de una persona[690] en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica» –artículo 3.1) Reglamento eIDAS–. Por su parte, el *sistema de identificación electrónica* vendrá constituido por el «[…] régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas o a una persona física que representa a una persona jurídica» –artículo 3.4) Reglamento eIDAS, entendiéndose por *medio de identificación electrónica* la «[…] unidad material y/o inmaterial que contiene los datos de identificación de una persona y que se utiliza para la autenticación en servicios en línea» –artículo 3.2) Reglamento eIDAS–. Se trata, en definitiva, de un régimen que conforma el total del proceso de identificación electrónica mediante la expedición de unidades que albergan datos de identificación y que posibilitan la autenticación transfronteriza[691].

---

[689] ALMONACID LAMELAS, V./ALAMILLO DOMINGO, I., «Los ciudadanos en el procedimiento y su personalidad electrónica: medios de identificación y firma», en CAMPOS ACUÑA, M. C. (coord.) *El nuevo procedimiento administrativo local tras la Ley 39/2015*, Las Rozas, Wolters Kluwer, 2016, pp. 210 y 211.

[690] Los *datos de identificación de una persona*, por su parte, se refieren al conjunto de datos (nombre, apellidos, número del DNI, etc.) que permite establecer la identidad de una persona, física o jurídica, o de una persona física que representa a una persona jurídica –artículo 3.3) Reglamento eIDAS–. En consecuencia, la identidad es aquello que posibilita a las personas físicas o jurídicas distinguirse en su individualidad, haciendo posible que una información se vincule o atribuya a esa concreta persona y, al tiempo, que se realice un manejo seguro y eficaz de los datos específicos y propios del sujeto; desde una perspectiva jurídica, la identidad será, a su vez, la base sobre la que se reconozcan derechos y obligaciones de las personas (MERCHÁN MURILLO, A., *Firma electrónica: funciones y problemática. Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, cit., p. 31).

[691] ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 703.

Por lo que respecta a estos sistemas de identificación electrónica, el artículo 7 RIE-SCTE establece las condiciones que habrán de satisfacer aquellos de estos sistemas que pretendan ser notificados con arreglo al artículo 9. Estas condiciones son las siguientes: a) que los medios de identificación electrónica en virtud del sistema de identificación hayan sido expedidos por el Estado miembro que efectúa la notificación, por su mandato o independientemente de dicho Estado miembro pero por él reconocidos; b) que los medios de identificación electrónica en virtud del sistema de identificación electrónica puedan usarse para acceder al menos a un servicio prestado por un organismo del sector público que exija la identificación electrónica en el Estado miembro que efectúa la notificación; c) que tanto el sistema de identificación electrónica como los medios de identificación electrónicos en su virtud expedidos cumplan los requisitos de al menos uno de los niveles de seguridad previstos en el acto de ejecución a que hace referencia el artículo 8.3; d) que el Estado miembro que efectúa la notificación garantice que los datos de identificación de la persona que representan en exclusiva a la persona en cuestión se atribuyen de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecido en el acto de ejecución a que se refiere el artículo 8.3, a la persona física o jurídica a la que se refiere el artículo 3.1), en el momento de expedición de los medios de identificación electrónica previstos en este sistema; e) que la parte que expide los medios de identificación electrónica previstos en este sistema garantice que los medios de identificación electrónica se atribuyan a la persona a que se refiere la letra anterior de conformidad con las especificaciones técnicas, las normas y los procedimientos del nivel de seguridad pertinente establecidos en el acto de ejecución a que se refiere el artículo 8.3[692]; f) el Estado miembro que efectúa la notificación garantiza la disponibilidad de la autenticación en línea de manera que cualquier parte usuaria establecida en el territorio de otro Estado miembro pueda confirmar los datos de identificación de la persona recibidos en formato electrónico, siendo preciso tener en cuenta, de un lado, que para las partes usuarias distintas de los organismos del sector público, el Estado miembro que efectúa la notificación podrá definir las condiciones de acceso a esa autenticación, debiendo ser la autenticación transfronteriza gratuita cuando se realice en relación con un servicio en línea prestado por un organismo del sector público, y, de otro, que los Estados

[692] Como dispone el artículo 11.2 del Reglamento, «[l]a parte que expida los medios de identificación electrónica será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de la letra e) del artículo 7 en una transacción transfronteriza».

miembros no impondrán requisitos técnicos específicos desproporcionados a las partes usuarias que tengan intención de llevar a cabo tal autenticación, cuando esos requisitos impidan u obstaculicen significativamente la interoperabilidad de los sistemas de identificación electrónica notificados[693]; g) al menos seis meses antes de la notificación a la que se refiere el artículo 9.1, el Estado miembro que efectúa la notificación presentará a los demás Estados miembros, a efectos de la obligación a que se refiere el artículo 12.5, una descripción de este sistema, de conformidad con las modalidades de procedimiento establecidas en los actos de ejecución a los que se refiere el artículo 12.7, y h) el sistema de identificación electrónica cumple los requisitos del acto de ejecución a que se refiere el artículo 12.8.

Una vez cumplidas tales condiciones, el Estado miembro que efectúa la notificación transmitirá a la Comisión la siguiente información y, sin dilaciones indebidas[694], cualquier modificación posterior de la misma (artículo 9 RIE-SCTE): a) una descripción del sistema de identificación electrónica, que incluya sus niveles de seguridad y el emisor o emisores de los medios de identificación electrónica en virtud de este sistema; b) el régimen de supervisión aplicable y la información sobre el régimen de responsabilidad respecto de la parte que expida los medios de identificación electrónica y la parte que utilice el procedimiento de autenticación; c) la autoridad o autoridades responsables del sistema de identificación electrónica; d) información sobre la o las entidades que gestionan el registro de los datos únicos de identificación de la persona; e) una descripción de cómo se cumplen los requisitos de los actos de ejecución a que se refiere el artículo 12.8; f) una descripción de la autenticación a la que se

[693] Por su parte, de acuerdo con el artículo 11.1 RIE-SCTE, «[e]l Estado miembro que efectúa la notificación será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de las letras d) y f) del artículo 7 en una transacción transfronteriza»; asimismo, añade el apartado tercero del precepto, «[l]a parte que realice el procedimiento de autenticación será responsable de los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en caso de incumplimiento de sus obligaciones en virtud de la letra f) del artículo 7 en una transacción transfronteriza». Todos los supuestos previstos en los apartados 1, 2 y 3 del artículo 11 Reglamento eIDAS se aplicarán con arreglo a las normas nacionales sobre responsabilidad, entendiéndose el contenido de lo en ellos dispuesto «[…] sin perjuicio de la responsabilidad de las partes de acuerdo con la legislación nacional en relación con una transacción en la que se utilicen medios de identificación electrónica incluidos en el sistema de identificación electrónica notificado en virtud del artículo 9, apartado 1».

[694] Término, este, jurídicamente indefinido y, pese a ello, muy repetido a lo largo de todo el texto de la norma.

refiere el artículo 7.f), y g) disposiciones relativas a la suspensión o revocación del sistema de identificación electrónica, o autenticación notificados o de las partes interesadas. La publicación en el DOUE de los sistemas de identificación electrónica notificados y la información básica al respecto tendrá lugar transcurrido un año desde la fecha de aplicación de los actos de ejecución a que hacen referencia los artículos 8.3 y 12.8 Reglamento eIDAS, encarnados en el REFEPTMNSMIE y en el REMI, respectivamente; ahora bien, si la Comisión recibe una notificación concluido el plazo anterior, publicará en el DOUE las modificaciones de la lista en el plazo de dos meses desde la fecha de recepción de la notificación. Asimismo, cualquier Estado miembro podrá presentar a la Comisión la solicitud de supresión de la lista de un sistema de identificación electrónica notificado en los términos *supra* expresados, llevándose a cabo por la Comisión la publicación en el DOUE de las modificaciones correspondientes en el plazo de un mes desde la fecha de recepción de la solicitud. Por último, la Comisión podrá, mediante actos de ejecución (a adoptar con arreglo al artículo 48.2 Reglamento eIDAS), definir las circunstancias, formatos y procedimientos relativos a la notificación apuntada; previsión esta que se ha plasmado en la DECFPN.

Para concluir, el artículo 12, apartados 1 a 4, RIE-SCTE establece la interoperabilidad de los sistemas de identificación electrónica. Para ello, se establecerá un marco de interoperabilidad que deberá cumplir las siguientes exigencias: a) aspirar a ser neutro desde un punto de vista tecnológico y no discriminar entre soluciones técnicas nacionales específicas para la identificación electrónica dentro del Estado miembro (principio de neutralidad tecnológica); b) ajustarse a las normas internacionales y europeas, siempre que sea posible; c) facilitar la aplicación del principio de privacidad desde el diseño, y d) garantizar que los datos personales se procesen con arreglo a la Directiva 95/46/CE. En concreto, el marco de interoperabilidad consistirá en lo siguiente: a) una referencia a los requisitos técnicos mínimos relativos a los niveles de seguridad contemplados en el artículo 8; b) una correlación entre los niveles de seguridad nacionales de los sistemas de identificación electrónica y los niveles de seguridad contemplados en el artículo 8; c) una referencia a los requisitos técnicos mínimos para la interoperabilidad; d) una referencia a un conjunto mínimo de datos de identificación de la persona que representan de manera única a una persona física o jurídica, y que está disponible en los sistemas de identificación electrónica; e) reglas de procedimiento; f) acuerdos para la resolución de litigios, y g) normas comunes de seguridad operativa. El 18 de septiembre de 2015 era la fecha máxima fijada para establecer las condiciones uniformes para la ejecución de los requisitos de interoperabilidad.

En lo que se refiere a la autenticación (o, términos propios, *identificación autenticada*), podemos entender por tal aquel servicio de seguridad que tiene por objeto corroborar la identidad alegada por un usuario participante en una sesión[695], o, en palabras del RIE-SCTE –artículo 3.5)–, aquel «[…] proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico»[696]. Los métodos de autenticación se suelen dividir en cuatro grandes categorías: a) algo que el usuario *sabe* (entre ellos, una contraseña, una frase o un número de identificación personal), b) algo que el usuario *tiene* (como una tarjeta de banda magnética o de circuito integrado), c) algo que el usuario *es* (como la huella dactilar, la geometría de la mano, el iris o el patrón de venas del fondo del ojo, la faz o la voz) y d) algo que el usuario *hace* (como la firma autógrafa, la cadencia de pulsación de las teclas o la velocidad en el manejo del ratón)[697]. En este sentido, la disponibilidad de la autenticación está prevista, como hemos podido ver, como una de las condiciones necesarias para la notificación de los sistemas de identificación electrónica, merced al artículo 7.f) RIE-SCTE.

---

[695] RIBAGORDA GARNACHO, A., «Seguridad informática», cit., p. 12.

[696] No es necesario, por tanto, que se den necesariamente estos tres elementos (esto es, autenticación de la entidad, autenticación del origen de los datos y autenticación de la integridad de los mismos) de forma simultánea. Sí parece, en cambio, que los dos últimos han de darse cumulativamente, pues, de lo contrario, la definición podría haber tenido la siguiente redacción: «[…] proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, del origen de datos en formato electrónico o de la integridad de los mismos» o «[…] proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica o del origen o la integridad de datos en formato electrónico».

[697] ALAMILLO DOMINGO, I., «Tipología legal de la firma electrónica en la Unión Europea», cit., p. 3; MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., p. 130. De este modo, como señala MERCHÁN MURILLO, A., *Firma electrónica: funciones y problemática. Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, cit., pp. 47 y 48, dos son los procesos fundamentales y consecutivos en orden a garantizar la identificación autenticada de una persona: en primer lugar, la identificación, es decir, «[…] el proceso necesario para la verificación de ciertos atributos de identidad de una persona y la emisión de una credencial de identidad, ligadas a esa persona para reflejar estos atributos» (este proceso estaría diseñado para responder a preguntas como ¿quién es usted?); en segundo lugar, la autenticación o proceso necesario «[…] para verificar a la persona que representa la credencial y, además, dice ser la persona descrita por esos atributos previamente verificados […] respecto a esa persona» (por su parte, este otro proceso estaría configurado para responder a cuestiones tales como ¿cómo se puede demostrar que usted es la persona que dice ser?).

De acuerdo con el artículo 10 del Reglamento eIDAS, si el sistema de identificación electrónica o la autenticación son violados o puestos parcialmente en peligro de tal forma que afecte a la fiabilidad de la autenticación transfronteriza de dicho sistema, el Estado miembro que efectúe la notificación suspenderá o revocará sin dilaciones indebidas dicha autenticación transfronteriza o las partes que resulten afectadas, debiendo informar al respecto a los demás Estados miembros y a la Comisión. De corregirse en el plazo de tres meses a partir de la suspensión o revocación la violación o puesta en peligro, el Estado miembro notificador restablecerá la autenticación transfronteriza e informará de esta circunstancia y sin dilaciones indebidas a los todos los demás Estados miembros y a la Comisión; de lo contrario, les comunicará la retirada del sistema de identificación electrónica. Las modificaciones correspondientes de la lista de los sistemas de identificación electrónica serán publicadas por la Comisión en el DOUE sin dilaciones indebidas.

1. Reconocimiento transfronterizo de los medios de identificación electrónica

Con el objetivo de garantizar el correcto funcionamiento del mercado interior, aspirando, al mismo tiempo, a conseguir un nivel de seguridad adecuado de los medios de identificación electrónica, el Reglamento eIDAS «[…] establece las condiciones en que los Estados miembros deberán reconocer los medios de identificación electrónica de las personas físicas y jurídicas pertenecientes a un sistema de identificación electrónica notificado de otro Estado miembro»[698]. Esta necesidad ya se venía plasmando en diferentes instrumentos legislativos, como la DSMI[699] o la DADPAST[700], ambas expresamente citadas en los considerandos 8 y 10 del Reglamento.

Tal y como detecta claramente la norma, el problema hasta ahora existente radicaba en la ausencia de reconocimiento mutuo por los Estados miembros de sus respetivos sistemas de identificación electrónica, lo que imposibilitaba, de facto, que un ciudadano europeo pudiera

[698] Y es que, como bien anticipa su considerando 12, «[u]no de los objetivos del presente Reglamento es eliminar las barreras existentes para el uso transfronterizo de los medios de identificación electrónica utilizados en los Estados miembros para autenticar al menos en los servicios públicos», concluyendo que «[…] lo que pretende es garantizar que sean posibles la identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros».

[699] DOUE L 376, de 27 de diciembre de 2006, p. 36.

[700] DOUE L 88, de 4 de abril de 2011, p. 45.

utilizar su identificación electrónica para autenticarse en un territorio distinto de aquel en el que residía. Urgente se antojaba, consecuentemente, poder contar con unos medios de identificación electrónica que fueran capaces de posibilitar interacciones electrónicas seguras a nivel transfronterizo. Y ello reconociendo, en todo momento, la libertad de tales Estados en materia de identificación electrónica, al establecer tan sólo un marco para que este reconocimiento sea posible; claro reflejo de lo anterior es el considerando 12 RIE-SCTE, que dispone, en lo que aquí interesa, que «[…] el presente Reglamento no se propone intervenir en los sistemas de gestión de la identidad electrónica e infraestructuras conexas establecidos en los Estados miembros», que será competencia exclusiva de cada uno de los mismos, de modo que, añade el considerando siguiente, «[…] los Estados miembros deben seguir siendo libres de utilizar o introducir, a efectos de identificación electrónica, medios de acceder a los servicios en línea. También deben poder decidir si interviene o no el sector privado en la prestación de estos medios. Los Estados miembros no deben estar obligados a notificar sus sistemas de identificación electrónica a la Comisión. Corresponde a los Estados miembros decidir si notifican todos, algunos o ninguno de los sistemas de identificación electrónica utilizados a nivel nacional para el acceso al menos a los servicios públicos en línea o a servicios específicos».

Lo anterior posibilitará la existencia de un panorama comunitario ciertamente diverso, donde podrá haber Estados miembros que introduzcan sistemas de identificación electrónica y que los notifiquen para su uso transfronterizo y Estados miembros que hagan lo propio pero sólo para su uso a nivel interno. Es por ello que, más que una base legal para la regulación de los sistemas de identificación electrónica (aspecto este contenido en la regulación a nivel nacional), el Reglamento eIDAS constituye resulta imprescindible para el reconocimiento mutuo entre los Estados miembros[701].

A la vista de cuanto precede, y de acuerdo con lo dispuesto por el artículo 6 del Reglamento, «[c]uando sea necesaria una identificación electrónica utilizando un medio de identificación electrónica y una autenticación en virtud de la normativa o la práctica administrativa nacionales para acceder a un servicio prestado en línea por un organismo del sector público[702]

[701] ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 698.

[702] Los organismos del sector público son definidos en el artículo 3.7 RIE-SCTE como «[…] las autoridades estatales, regionales o locales, los organismos de Derecho público y las asociaciones formadas por una o varias

en un Estado miembro, se reconocerá en dicho Estado miembro, a efectos de la autenticación transfronteriza en dicho servicio en línea, el medio de identificación electrónica expedido en otro Estado miembro, siempre que: a) este medio de identificación electrónica haya sido expedido en virtud de un sistema de identificación electrónica incluido en la lista publicada por la Comisión de conformidad con el artículo 9[703]; b) el nivel de seguridad de este medio de identificación electrónica corresponda a un nivel de seguridad igual o superior al nivel de seguridad requerido por el organismo del sector público para acceder a dicho servicio en línea en el primer Estado miembro, siempre que el nivel de seguridad de dicho medio de identificación electrónica corresponda a un nivel de seguridad *sustancial* o *alto*[704], y c) el organismo público en cuestión utilice un nivel de seguridad *sustancial* o *alto* en relación con el acceso a ese servicio en línea»[705]; este reconocimiento deberá producirse, como muy tarde,

---

de estas autoridades o uno o varios de estos organismos de Derecho público, o las entidades privadas mandatarias de al menos una de estas autoridades, organismos o asociaciones para prestar servicios públicos actuando en esa calidad».

[703] Para lo cual es necesario que haya sido previamente notificado por el Estado miembro en los términos establecidos por la DECFPN. En cualquier caso, para que un sistema de identificación electrónica sea objeto de notificación, es preciso que cumpla todas las condiciones establecidas en el artículo 7 RIE-SCTE, ya descrito.

[704] De este modo, entiendo, de la letra b) del artículo 6.1 RIE-SCTE se desprenden dos alternativas igualmente posibles: 1) si un organismo público del Estado miembro *A* requiere en su respectivo territorio un medio de identificación electrónica con un nivel de seguridad *sustancial* para acceder a un servicio en línea, sólo se deberá reconocer en dicho Estado miembro un medio de identificación expedido en el Estado miembro *B* si el nivel de seguridad del medio de identificación en este último territorio expedido es *sustancial* o *alto*; 2) si un organismo público del Estado miembro *A* requiere en su respectivo territorio un medio de identificación electrónica con un nivel de seguridad *alto* para acceder a un servicio en línea, sólo se deberá reconocer en dicho Estado miembro un medio de identificación expedido en el Estado miembro *B* si el nivel de seguridad del medio de identificación en este último territorio expedido es *alto*.

[705] Como bien indica *Ibid.*, pp. 706 y 707, sorprende que, en este punto, el Reglamento excluya la posibilidad de que una persona que cuente con un sistema de identificación electrónica mejor que el requerido no pueda emplearlo; es esto lo que sucederá, por ejemplo, con un ciudadano español que pretenda emplear su DNIe para acceder a un servicio en otro Estado miembro que únicamente requiera contraseña (y de baja calidad). A juicio de este autor, que compartimos, «[s]e trata de una restricción contraria a la lógica –parece que debería aplicar el principio de que "quien puede lo más, puede lo menos"– y que sólo puede entenderse, en mi opinión, desde el punto de vista presupuestario; es decir, para no obligar a ese Estado miembro a incorporar ninguna autenticación transfronteriza a ese servicio», dado que, como veremos a continuación, no es obligatorio el reconocimiento de los sistemas de identificación electrónica de nivel bajo.

doce meses después de que la Comisión publique la lista a que se refiere el artículo 9, no aplicándose el reconocimiento transfronterizo, en ningún caso, antes de septiembre de 2018[706]. En cualquier caso, lo antes expuesto no será óbice para que un medio de identificación electrónica expedido por un sistema de identificación electrónica incluido en la lista publicada por la Comisión de acuerdo con este último precepto y que corresponda al nivel de seguridad bajo pueda ser reconocido por los órganos del sector público a efectos de autenticación transfronteriza del servicio prestado en línea por dichos órganos.

Ha sido el artículo 8 del Reglamento eIDAS el encargado de establecer la distinción entre estos tres niveles de seguridad, que se identifican con el nivel *bajo*, *sustancial* y *alto*. En primer lugar, el nivel de seguridad *bajo* corresponderá a un medio de identificación electrónica que establezca un grado limitado de confianza en la identidad pretendida o declarada de una persona y se describirá en referencia a las especificaciones técnicas, las normas y los procedimientos del mismo, entre otros los controles técnicos; su objetivo será el de reducir el riesgo de uso indebido o alteración de la identidad. En segundo lugar, el nivel de seguridad *sustancial* será aquel que posea un medio de identificación electrónica que imprima un grado sustancial de confianza en la identidad pretendida o declarada de una persona, en relación con las especificaciones técnicas, las normas y los procedimientos establecidos; en este caso, el objetivo radicará en disminuir sustancialmente el riesgo del uso indebido o alteración de la identidad. En tercer y último lugar está el nivel de seguridad *alto*, se atribuirá a aquel medio de identificación electrónica que imponga un alto grado de confianza en la identidad pretendida o declarada de una persona, superior al medio de identificación electrónica *sustancial*, también en función de las especificaciones técnicas, las normas y los procedimientos establecidos; aquí, el objetivo perseguido no será ya el de reducir sino, tanto más, el de evitar el uso indebido o la alteración de la identidad[707].

---

[706] Artículo 52.3 RIE-SCTE.

[707] Sobre esta cuestión, *vid.* GONZÁLEZ MORENO, M., «¿Qué se ha de tener en cuenta a la hora de implantar servicios de identificación y firma electrónica?», *Actualidad jurídica Aranzadi*, vol. 923, 2016, pp. 1 y 2. De definir las especificaciones y los procedimientos técnicos en virtud de los cuales se concretarán los niveles de seguridad *bajo*, *sustancial* y *alto* de los medios de identificación electrónica expedidos en el marco de un sistema de identificación electrónica notificado se ha encargado el REFEPTMNSMIE (punto 2 del anexo). Y lo ha hecho por medio de la determinación de la fiabilidad y la calidad del procedimiento para demostrar y comprobar la identidad de las personas físicas o jurídicas que solicitan la expedición de los medios de identificación electrónica,

## 2. El Documento Nacional de Identidad electrónico como medio de identificación electrónica preeminente en la normativa española tradicional

En nuestro país, una de las grandes novedades que trajo consigo la entrada en vigor de la LFE[708] fue, precisamente, el establecimiento de las bases para la regulación del DNIe[709].

Su nacimiento viene a cubrir la necesidad, por parte del sector público, de otorgar identidad personal a los ciudadanos para su empleo en la nueva sociedad de la información, fomentando la dinamización del comercio electrónico[710]. Resulta innegable que el DNIe constituye la principal estrategia española sobre identificación electrónica[711], estrategia que se ha

---

del procedimiento para expedir los medios de identificación electrónica solicitados, del mecanismo de autenticación mediante el cual la persona física o jurídica utiliza los medios de identificación electrónica para confirmar su identidad a una parte usuaria, de la entidad que expide los medios de identificación electrónica y de cualquier otro organismo que intervenga en la solicitud de expedición de los medios de identificación electrónica y de las especificaciones técnicas y de seguridad de los medios de identificación electrónica. En principio, todos los elementos correspondientes a un mismo nivel de seguridad deberán cumplirse para coincidir con el nivel de seguridad reclamado

[708] GONZÁLEZ DE ALAIZA CARDONA, J. J. Y OTROS, «Los contratos de adhesión y la contratación electrónica», cit., p. 1794; MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 273; MERCHÁN MURILLO, A., *Firma electrónica: funciones y problemática. Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, cit., p. 73; MORENO DELGADO, M. Y OTROS, «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», cit., p. 211.

[709] Integrado inicialmente en el conjunto de iniciativas del conocido como *Plan de Acción INFO XXI* y, con posterioridad, en el *Plan de Choque para el impulso de la Administración Electrónica*, dentro del programa *administración.es* del *Plan de Actuaciones para el desarrollo de la Sociedad de la Información en España* "*España.es*".

[710] GRUPO DE TRABAJO DE COMUNICACIÓN Y DIVULGACIÓN, *DNI electrónico: guía de referencia básica*, Madrid, Comisión Técnica de Apoyo a la Implantación del DNI electrónico, 2014, p. 3; VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., p. 180.

[711] Como señala VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», cit., p. 160, «[d]e todos los medios de acreditación personal que hay hoy en día, el más generalizado, el que acapara la confianza de todos, es el Documento Nacional de Identidad; por ello, si dicho DNI incorpora la clave privada de un certificado electrónico, expedido por las autoridades policiales conforme a la tecnología más moderna y segura, no cabe duda de que estaremos ante un instrumento capaz de dinamizar el tráfico electrónico y de acaparar mayores dosis de seguridad jurídica».

complementado, bien es cierto, con otros medios, como el proyecto CERES de la FNMT-RCM o el recientemente aprobado sistema Cl@ve[712].

El DNIe es la versión electrónica del DNI y se encuentra actualmente regulado en los artículos 15 y 16 y en la D. A. 6ª LFE, norma que, hasta tanto sea derogada (en principio, y presumiblemente, por los artículos 8 y 9 ALSEC) se verá complementada, por mandado del apartado primero de la D. F. 2ª LFE, con el RDEDNI-CFE[713] y, en general, con el propio Reglamento eIDAS, con la LOPDCP, con el RDRDLOPDCP (estas dos últimas, pendientes de derogación en favor del RPPFTDP), con la LOPSC[714] y con la OADPPCMI[715]. De acuerdo con el artículo 15.1 LFE (en términos idénticos, artículo 8.1 ALSEC), el DNIe es el DNI[716] «[…] que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos[717]»; se trata, por tanto, de un certificado electrónico llamado

[712] ALMONACID LAMELAS, V. Y OTROS, «Los ciudadanos en el procedimiento y su personalidad electrónica: medios de identificación y firma», cit., p. 211.

[713] Este Real Decreto se ha visto modificado sucesivamente por el PRDMRDEDNI-CFE –BOE núm. 265, de 3 de noviembre de 2009–, por el SRDMRDEDNI-CFE –BOE núm. 281, de 23 de noviembre de 2013– y por el TRDMRDEDNI-CFE –BOE núm. 129, de 30 de mayo de 2015–.

[714] BOE núm. 77, de 31 de marzo de 2015.

[715] BOE núm. 64, de 16 de marzo de 2006. Esta Orden se ha visto posteriormente modificada por la OMOAD-PPCMI (BOE núm. 92, de 17 de abril de 2015).

[716] De acuerdo con el artículo 8.1.2º LOPSC, el DNI «[e]s un documento público y oficial y tendrá la protección que a éstos otorgan las leyes, así como suficiente valor por sí solo para la acreditación de la identidad y los datos personales de su titular», estableciendo, como bien un régimen público y monopolístico reservado al Ministerio del Interior, que lo ejerce a través de la Dirección General de la Policía.

[717] De este modo, como bien hacen constar MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., p. 167, más que definir al DNIe, el precepto enuncia las dos funciones principales que desempeña: medio acreditativo de la identidad de su titular e instrumento de firma electrónica. Por lo demás, no se explicita en la LFE que la firma electrónica empleada haya de ser reconocida, pese a ello, son varios los autores que entienden que así deberá ser: CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 174, sostiene que esta postura «[…] teniendo en cuenta la importante medida de seguridad que supone la utilización de una tarjeta inteligente», si bien añade la necesidad de que se cumplan todos los requisitos del artículo 3.3 LFE, a excepción de la garantía del artículo 20.2 LFE; MENÉNDEZ MATO, J. C. Y OTROS, *Derecho e informática: ética y legislación*, cit., pp. 168 y 169, entienden que «[…] dicha conclusión puede ser […] alcanzada si se atiende a los términos empleados en los artículos 15.2 y 16.1 de la Ley española 59/2003 de firma electrónica. El primero de estos preceptos hace expresa referencia

a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma autenticidad e integridad que la que tienen aquellas comunicaciones convencionales realizadas a través de medios físicos[718]. Seguidamente (también, artículo 8.2 ALSEC), se establece el deber de todas las personas, físicas y jurídicas, públicas y privadas, de reconocer la eficacia del DNIe para acreditar la identidad y los demás datos personales del titular que en él consten, así como para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos[719].

---

a la necesidad de que, como resultado del empleo de la firma electrónica que recoge el documento nacional de identidad, se acredite la identidad del firmante y la integridad de los documentos firmados mediante su utilización. Esta última puntualización es la que permite exigir al menos que la firma sea avanzada, ya que el empleo de una simple firma electrónica no avanzada del tipo *username/password* o de un PIN no garantizaría la integridad del contenido del documento y su no manipulación por terceros. El artículo 16 –titulado: *Requisitos y características del documento nacional de identidad electrónico*– señala en su apartado primero que "los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20". Precisamente su contenido permite alcanzar la conclusión de que la firma electrónica propia del documento de identidad electrónico –además de tratarse de una firma avanzada– será también reconocida»; SANJURJO REBOLLO, B., *Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, protección de datos, negocios audiovisuales, e-commerce, consumidores, marketing*, cit., p. 520, afirma con rotundidad que la firma electrónica realizada a través del DNIe tendrá «[…] el mismo valor que la firma manuscrita respecto de los datos consignados en forma electrónica». En contra, ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 35, quien defiende que «[…] el DNI no produce la firma electrónica reconocida, porque no impone el necesario dispositivo seguro de creación de firma de la firma electrónica reconocida y, sin embargo, se le dota de la mayor eficacia jurídica, lo que es ilógico desde la óptica jurídica».

[718] GONZÁLEZ DE ALAIZA CARDONA, J. J. Y OTROS, «Los contratos de adhesión y la contratación electrónica», cit., p. 1794; PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, Cizur Menor, Aranzadi, 2013, p. 471; VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., p. 154.

[719] Este deber legal ha llevado a ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 35, a afirmar con rotundidad lo siguiente: «[…] sólo con el DNI electrónico se afecta de forma absoluta al mercado de servicios de certificación, aunque también es cierto que la existencia del DNI "en papel" no ha afectado a la existencia de tarjetas de identidad, públicas o privadas, si bien éstas tienen unas funciones y modelos de negocio diferentes, y no acceden a un mercado tan abierto y rápido como son las relaciones jurídicas a través de los medios telemáticos. Nos encontramos ahora, sin embargo, ante una clara invasión competencial del mercado por parte del sector público, aprovechando un título competencial incorrecto. La reserva que se realiza al Estado en materia del DNI se encuentra conectada con la

Pese a ello, no parece que pueda defenderse la existencia de una obligación general de admitir su uso[720].

Así las cosas, este DNIe, que irá sustituyendo de forma paulatina al tradicional, aúna en un único documento las funciones del DNI (acreditación de los datos en él consignados mediante la presentación física) con otras nuevas, como la identificación del usuario en redes electrónicas y la firma electrónica de documentos, que serán las dos funciones esenciales del mismo[721]. Esta diferenciación tiene su reflejo en el mismo formato, de modo que, a pesar de

---

identificación de los nacionales españoles, no con su capacidad de firma. No queda más remedio que indicar que la configuración actual del DNI viola la Constitución española y la libertad de empresa en el marco de una economía de mercado que reconoce, además de toda la normativa comunitaria y estatal de defensa de la competencia, creando un monopolio de hecho absolutamente prohibido. Al mismo tiempo, el DNI electrónico puede suponer un ataque a la libertad e intimidad personales y a la protección de datos, al existir una única base de datos impuesta legalmente, que supondría la existencia de un identificador único, frente a la situación actual de dispersión de datos del ciudadano entre las distintas Administraciones públicas»; en la misma línea, CRUZ RIVERO, D., «El DNI electrónico y el mercado de entidades de certificación», *Revista de la contratación electrónica*, vol. 69, 2006, p. 27, quien sostiene que la existencia de un DNIe válido para todo tipo de usos, habida cuenta de que, *de facto*, es utilizado para prácticamente todo, comporta un inconveniente para los PSSIic privados que se dedican a la emisión de certificados como actividad empresarial, o MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 279, al afirmar que «[…] la existencia de un DNI electrónico válido para todo tipo de usos, sin limitación cualitativa alguna, aun cuando pudiera resultar útil para el ciudadano, puede resultar inconveniente para los prestadores de servicios de certificación privados que se dedican a la emisión de certificados como actividad empresarial. La coexistencia de estos operadores privados con una autoridad de certificación pública que emite certificados altamente fiables, admisibles para usos generales y probablemente gratuitos o de bajo coste para el solicitante, puede resultar cuanto menos problemática desde el punto de vista empresarial, mientras que desde el punto de vista jurídico habría de analizarse su incidencia en los principios legales (de origen comunitario) que consagran la libre competencia en el mercado de los prestadores de servicios de certificación».

[720] ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», cit., p. 683.

[721] CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., p. 172. Este autor sostiene, incluso, que, en la práctica, es posible que las funciones de identificación y firmado puedan llegar a unirse; en concreto, dispone que «[…] ciertamente, estas funciones se presentan separadas, de modo que el firmado exige la puesta en marcha del procedimiento de cifrado utilizando los datos de creación de firma insertos en el chip del DNI. Pero cuando el titular del DNI se identifique antes de presentar un documento y el receptor sea capaz de registrar de forma vinculada con ese documento la utilización previa del DNI, el resultado será muy parecido, si no idéntico, a la firma. En concreto,

seguir consistiendo en una tarjeta de policarbonato en la que constan los mismos datos que en el DNI (bien es cierto que la fotografía, la huella dactilar y la firma manuscrita se hallan digitalizados), incluye un chip que recogerá el certificado electrónico para autenticar la personalidad del ciudadano, el certificado para firmar electrónicamente y las claves de cifrado y de descifrado[722]. En este sentido, tal y como establece el artículo 12.1 RDEDNI-CFE tras la reforma operada en 2015, la vigencia de los certificados electrónicos reconocidos incorporados al DNIe no podrá ser superior a cinco años, mientras que, con carácter general, el DNI tendrá un período de validez, a contar desde la fecha de expedición o de cada una de sus renovaciones (6.1 RDEDNI-CFE), de dos años, cuando el solicitante no haya cumplido los cinco años de edad; de cinco, cuando el titular haya cumplido la edad anterior y no haya alcanzado los treinta al momento de la expedición o renovación; de diez, cuando el titular haya cumplido los treinta años y no haya alcanzado los setenta, y permanente, cuando el titular haya cumplido los setenta años; en consecuencia, para aquellos casos en que la vigencia del certificado electrónico sea inferior a la del DNI, este mismo precepto prevé la posibilidad de solicitar nuevos certificados reconocidos, manteniendo la vigencia del DNI durante el tiempo que reste.

Por la función de seguridad pública que cumple el DNIe, ambas funciones, identificativa y de firmado, serán certificadas por una autoridad de certificación electrónica propia, dependiente del Ministerio del Interior, a través de la Dirección General de Policía, imprimiendo, pues, mayores dosis de confianza en los ciudadanos a la hora de realizar interacciones electrónicas[723]. Dicha entidad de certificación estará obligada a cumplir las obligaciones que la LFE impone a los PSSIc que expidan certificados electrónicos reconocidos, «[…] con excepción de la relativa a la constitución de la garantía a que se refiere el apartado 2 del artículo

---

entendemos que podría utilizarse este sistema para la presentación telemática de documentos a la Administración. Este procedimiento equivaldría, en soporte papel, a la sustitución de la firma en el documento de quien lo presenta por una declaración del funcionario que lo recibe certificando que quien lo ha presentado ha mostrado su DNI y es quien dice ser. Tal acto no existe en soporte papel. En nuestra opinión, en estos casos, será firma electrónica, aunque no reconocida, la identificación como suscriptor del documento que se incluya en el propio documento (al pie del mismo, por ejemplo), mientras que el DNI electrónico se habrá utilizado como una simple medida de seguridad, sin perjuicio del valor probatorio que ésta pueda tener».

[722] ROVIRA FERRER, I., «El DNI electrónico: un análisis crítico y global», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 26, 2011, p. 2.

[723] DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 539.

20[724]» (artículo 16.1 LFE); en este punto, el Anteproyecto de Ley –artículos 9 y 11.3.b) AL-SEC– introduce dos importantes novedades respecto de la norma a la que pretende sustituir: en primer lugar, reduce el importe mínimo total a que ha de ascender el seguro de responsabilidad civil para afrontar el riesgo de responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados electrónicos que expidan, que pasaría de 3.000.000,00 € a 1.500.000,00 €; en segundo lugar, y derivado de la incorporación legal de nuevos servicios de confianza, establece que, caso de que el PSSIisc preste más de uno, se añadirá un importe de 500.000,00 € más por cada servicio de confianza adicional que preste. Por lo demás, añade el artículo 16.2 LFE que «[…] la Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados».

## II. ESTRUCTURA TRIANGULAR DEL SISTEMA DE FIRMA ELECTRÓNICA

El funcionamiento de la firma electrónica, dentro de la dinámica contractual, reposa sobre la base de tres pilares o elementos subjetivos fundamentales (**anexo XVII**): el firmante, el tercero que confía y el PSSIisc, PSSIisc que, a su vez, pertenecerá a la categoría más general del PSSIi (**anexo XVI**).

[724] «Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan. La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros. Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto». En opinión de autores como FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 74 y ROVIRA FERRER, I., «El DNI electrónico: un análisis crítico y global», cit., p. 7, esta exención, aun cuando sea evidente que el Estado no ha de prestar garantías ante sí mismo, provoca claras desigualdades, pues, si ya es suficientemente devastadora la introducción de la actuación de un Ministerio en un ámbito de libre competencia, aún lo es más si esta se permite adicionando la utilización de sus privilegios y no en sede de igualdad.

## 1. Firmante

De acuerdo con el artículo 3, apartado 9), RIE-SCTE, firmante será la persona física que crea la firma electrónica[725]; es decir, aquella persona que, dentro del sistema de criptografía asimétrica dominante, se encuentra en posesión de las claves, privada y pública, con la que encriptar (por él mismo, con el dispositivo de creación de firma electrónica), primero, y desencriptar (por el tercero que confía, con el dispositivo de verificación de firma electrónica), después, el mensaje de datos. Vemos reducirse, entendemos que correctamente, la redundante, extensa e innecesaria definición descriptiva contenida en el artículo 2.3) de la Directiva precedente –también, en términos prácticamente idénticos, en los artículos 2.c) RDLFE[726],

[725] Definición, esta, prácticamente idéntica a la presentada inicialmente por la Comisión con ocasión de la definición de firmante dentro de la DFE, en virtud de la cual este sujeto venía personificado en aquella «[…] persona que crea una firma electrónica». En el Derecho italiano, la figura del firmante (*titular*, bajo su denominación) es definida en el artículo 1.aa) CAD como «[…] la persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica», o, lo que es lo mismo, «[…] la persona física a la que es atribuida la firma electrónica y que tiene acceso a los dispositivos para la creación de la firma electrónica».

[726] «[…] la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa». Esta definición es, de todas las citadas, la más diferente, en cuanto que, en primer lugar, la figura, al igual que vuelve a suceder con el RIE-SCTE, se ciñe exclusivamente a las personas físicas (con la única excepción del artículo 5.3, *in fine*, RDLFE, que, únicamente a efectos de cumplimiento de las obligaciones tributarias, admitía la posibilidad de que el signatario fuera una persona jurídica), entrando en abierta contradicción con la postura más amplia de la DFE a la que pretende adaptarse aun antes de la promulgación de esta, DFE que, si bien no admite expresamente esta posibilidad, tampoco la excluye; en segundo lugar, porque quien firma electrónicamente recibe el nombre de *signatario*, en lugar del de *firmante*. En relación con este último aspecto, se consigue, por tanto, la unificación definitiva de términos y se separan y clarifican los ámbitos subjetivos de aplicación en materia de firma y sello electrónicos entre la norma europea y la norma nacional, acabando con una contradicción ya existente desde antes de la LFE, expresada por autores como ORDUÑA MORENO, F. J., *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, pp. 136 y 137, en los siguientes términos: «[…] La Directiva y el proyecto de Ley Modelo de la CNUDMI/UNCITRAL utilizan el término firmante. El RDL 14/1999, sin embargo, utiliza el término signatario. En el proyecto de Ley Modelo se ha planteado la posibilidad de utilizar la expresión "titular de …" (los datos o dispositivo de creación de firma). Es una cuestión de matiz. Se trata de enfatizar el hecho de ser titular o "tenedor" único de una clave privada, con independencia de su efectivo uso o no, o bien incidir en el hecho de la efectiva utilización del instrumento de firma y la consiguiente generación de un documento electrónico efectivamente cifrado, esto es, firmado. El RDL define al "signatario" como la persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa. El legislador español lleva a cabo una restricción respecto del texto de la Directiva. Ésta define al "firmante" como la persona

2.d) LMFE[727] y 6.2 LFE[728]–, que entendía por tal «[…] la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o

que está en posesión… Incluye, pues, tanto a persona física como a jurídica. La norma general en el ordenamiento jurídico privado español sólo permite que la persona física, no la jurídica, sea titular de firmas electrónicas. Es una opción de política legislativa: se sigue el modelo de la firma manuscrita (sólo la tienen las personas físicas). Sin perjuicio del principio de la equivalencia funcional (seguido por la Ley Modelo), hay que tener presente que las nuevas tecnologías permiten opciones y posibilidades nuevas. Una persona jurídica no puede firmar con la mano por la sencilla razón de que carece de ella, como no puede realizar absolutamente nada en sentido material. Pero ahí está la ficción jurídica de la personalidad. La persona jurídica actúa a través de personas físicas, pero las consecuencias jurídicas se imputan a la persona jurídica. ¿Por qué si técnicamente es posible imputar una firma electrónica a una persona jurídica no se ha de poder hacer así? En términos reales, ¿qué diferencia hay entre imputar las consecuencias jurídicas de la firma o la firma en sí, si en todo caso técnicamente es posible conocer la persona física que lleva a cabo la efectiva "plasmación" de la firma (encriptación) –la haya aplicado directamente o no–? De hecho, a efectos fiscales parece, desde luego, más operativo otorgar una firma electrónica al ente o persona jurídica, que tiene su correspondiente código de identificación fiscal (CIF)».

[727] «[…] la persona que posee los datos de creación de la firma y que actúa por cuenta propia o por cuenta de la persona a la que representa». Discutible es la ubicación sistemática de este apartado, justo a continuación, y en el mismo precepto, que aquel que contiene la definición de certificado electrónico, aun a sabiendas de que el firmante puede firmar electrónicamente sin que esta firma electrónica conste de certificado, por no mencionar el nombre («certificados electrónicos») del Título II en el que se inserta.

[728] «[…] la persona que utiliza un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa»; a favor de esta definición y del empleo del término *firmante*, *vid.* FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, cit., p. 71. Con la LFE se reconocía abiertamente la posibilidad, ya intuida en la DFE, de que el firmante pudiera ser persona jurídica; así lo hace la Exposición de Motivos de la norma, que se expresa en los siguientes términos: «[…] asimismo, otra novedad es el establecimiento en la ley del régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático. Se va así más allá del Real Decreto Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ello haya representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales»; a favor de esta nueva posibilidad, *vid.* MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., p. 137, que sostiene lo siguiente: «[…] una persona jurídica no puede firmar con la mano por la sencilla razón de que carece de ella, como no puede realizar absolutamente nada en sentido material. Pero ahí está la ficción jurídica de la personalidad. La persona jurídica actúa a través de personas físicas, pero las consecuencias jurídicas se imputan a la persona jurídica. ¿Por qué si técnicamente es posible imputar una firma electrónica a una persona jurídica no se puede hacer así?»; en la misma línea, *vid.* MORENO DELGADO, M. Y OTROS, «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en

persona física o jurídica a la que representa»; aspectos, todos ellos, que pueden inferirse por deducción de la definición proporcionada por el nuevo Reglamento. Por lo demás, de forma cumulativa o no, la noción de firmante podrá verse acompañada de otros términos; así sucede en la práctica jurídica, técnica y comercial con los nombres de *solicitante*, *titular* o *suscriptor*, en aquellos casos en que la firma electrónica se vea acompañada de certificado o, en general, con otros relacionados, como los de *poseedor de la clave*, *responsable de la custodia* o *firmante material*, generándose, con frecuencia, una cierta confusión derivada del empleo de múltiples denominaciones para una misma figura[729].

De este modo, y como novedad más importante en este punto, desaparece con el RIESCTE la mención a una posibilidad específica contemplada en la normativa anterior y que ahora hemos de entender suprimida[730]. Nos estamos refiriendo a la posibilidad de que el

---

relación al Real Decreto-ley 14/1999», cit., p. 205. En contra, *vid.* VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., p. 139, opinión reiterada de nuevo en la obra VEGA VEGA, J. A., *Derecho mercantil electrónico*, cit., p. 165.

[729] MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 139. ALAMILLO DOMINGO, I. Y OTROS, «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 23, establecen, sin embargo, que, «[…] para dotar de mayor seguridad jurídica a las diferentes situaciones que se pueden producir en el tráfico jurídico, sería conveniente que cada una de las posibles situaciones fuera reconocida y regulada al margen de las restantes, clarificando al mismo tiempo la utilización de la firma electrónica». Por ello, añaden, hubiera sido conveniente definir y regular, cuanto menos, las figuras del *solicitante*, como la persona que, en nombre propio o en representación de otro, solicita un certificado; *suscriptor*, como la persona física o jurídica identificada en el certificado y que dispone del derecho de uso de dicho certificado para generar firmas basadas en el mismo, y *firmante*, como la persona física que, en nombre propio o en representación de otro, emplea directamente o dispone del control de la utilización de un dispositivo de creación de firmas imputables a un suscriptor de certificado, defendiendo, por tanto, un modelo de roles segregados frente al modelo existente de rol único y apostando, así, a favor del primero, «[…] en el que el solicitante, suscriptor y firmante recibieran un tratamiento diferente, apropiado a sus funciones en relación con los procedimientos de firma electrónica, que de momento no ha sido acogido por nuestro legislador». Sobre esta distinción, *vid.* también GONZÁLEZ NAVARRO, F., «Comentario al art. 45 de la Ley de régimen jurídico de las Administraciones públicas y procedimiento administrativo común», cit., pp. 22 a 29.

[730] No obstante, ya por entonces, autores como ALAMILLO DOMINGO, I., «Tipología legal de la firma electrónica en la Unión Europea», cit., p. 29, afirmaban que «[e]n el caso de la firma electrónica reconocida, en nuestra opinión, y en contra de otra doctrina, el firmante debe ser una persona física, aunque no debe ser necesariamente el titular o suscriptor del certificado, que puede ser perfectamente una persona jurídica, en cuyo caso el firmante es el poseedor de la clave privada de firma del suscriptor, con la correspondiente autorización, expresa o tácita. Sólo cuando se puede vincular un mensaje con un poseedor de una clave privada que es una persona

firmante pueda ser persona jurídica, figura que ahora se ve reemplazada por otra hasta ahora desconocida en el plano normativo: el conocido como *creador de un sello*[731] –apartado 24) del artículo 3 RIE-SCTE–, que exigirá una nueva adaptación normativa que suponga la derogación implícita de cuantos preceptos no contemplen esta separación en la LFE –entre otros, los artículos 7 y 11.2.e)–.

Junto a lo anterior, hemos de detenernos en otro aspecto no menos relevante. A tenor de las definiciones proporcionadas por el RIE-SCTE respecto de las nociones de *firmante*, de *firma electrónica* y de *identificación electrónica*, podemos extraer las siguientes conclusiones: en primer lugar, firmante es la persona física que crea una firma electrónica; en segundo lugar, y como en su momento expusiéramos, parece adecuado realizar una reinterpretación de la noción de firma electrónica general que proporciona el Reglamento, en el sentido de entender que el mínimo denominador común que toda firma electrónica ha de tener es el de servir como medio de identificación electrónica del firmante, en línea con la normativa comunitaria y nacional anterior; en tercer y último lugar, la identificación electrónica, aplicada a la firma electrónica, es definida como el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o a una persona física que representa a una persona jurídica. Ahora bien, no se contempla la posibilidad de que una persona física pueda representar a otra persona física (tampoco, aunque este no sea el debate seguido en el presente estudio, que una persona jurídica pueda representar a otra persona jurídica, ficción que, pese a ser compleja, también resultaría factible en la práctica[732]), opción esta que sí estaba expresamente prevista en las nociones de firmante del RDLFE, de la DFE y de la LFE. Este problema parece subsanarse en nuestro país con el artículo 5.1.a) ALSEC, que, al hablar de la extinción de la vigencia de los certificados electrónicos mediante

---

física, y que además ha conocido y aceptado el contenido del mensaje, se puede hablar propiamente de una firma electrónica que es equivalente a una firma manuscrita; es decir, se trata de un requisito de la firma electrónica reconocida. Por el contrario, la firma electrónica realizada por una máquina o por un dispositivo bajo el control de una persona jurídica será, a lo sumo, una firma electrónica avanzada, que como sabemos, no se equipará directamente a la firma manuscrita».

[731] Es decir, la persona jurídica que crea un sello electrónico.

[732] En la misma línea, MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, cit., p. 142, al afirmar que «[…] en el comercio tradicional una persona jurídica puede actuar en nombre y representación de otra persona jurídica (situación que, sin embargo, en el ámbito del comercio electrónico puede suponer una cierta complejidad práctica)».

revocación, dispone expresamente que esta podrá producirse, entre otras, por la «[s]olicitud formulada por el firmante, *la persona física o jurídica representada por éste*, un tercero autorizado, el creador del sello o el titular del certificado de autenticación de sitio web»[733], previendo, pues, aun de manera indirecta, esta posibilidad y contradiciendo, en consecuencia, aquello que el Reglamento eIDAS, no entendemos bien por qué, no contempla de manera explícita. En consecuencia, entendemos que lo más adecuado, más allá de la eventual promulgación en España de lo que ahora es un Anteproyecto de Ley, sería la modificación del RIE-SCTE en este punto concreto, añadiendo a los apartados 1), 3) y 4) del artículo 3 esta ampliación en los supuestos de representación, en una suerte de definiciones que podrían quedar como siguen:

> *1) "identificación electrónica", el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica, a una persona física que representa a una persona jurídica o a otra persona física o a una persona jurídica que representa a una persona física o a otra persona jurídica*; *3) "datos de identificación electrónica de la persona", un conjunto de datos que permite establecer la identidad de una persona física o jurídica, de una persona física que representa a una persona jurídica o a otra persona física o de una persona jurídica que representa a una persona física o a otra persona jurídica,* y *4) "sistema de identificación electrónica", un régimen para la identificación electrónica en virtud del cual se expiden medios de identificación electrónica a las personas físicas o jurídicas, a las personas físicas que representan a personas jurídicas o a otras personas físicas o a personas jurídicas que representan a personas físicas o a otras personas jurídicas.*

Por último, y dentro de la dinámica propia del contrato electrónico, hemos de dejar constancia de un hecho obvio pero, a la vez, relevante. Nos estamos refiriendo a la posibilidad de que el firmante adopte tanto el rol del PSSI como el del DSSI; en consecuencia, y dependiendo del caso, tendremos que remitirnos a todo cuanto se ha expuesto respecto de uno u otro a lo largo del presente estudio, siendo de aplicación cumulativa los derechos, obligaciones y responsabilidades generales propias de la parte activa o pasiva del contrato electrónico, junto con aquellas específicas propias de su condición de firmante de dicho documento. Lo mismo sucederá con la figura del tercero que confía en la firma electrónica del firmante.

2. Tercero que confía

Dentro del sistema triangular que tradicionalmente conforma la firma electrónica, la contraparte principal del firmante viene representada por la figura del tercero que confía. Ha

[733] La cursiva es propia.

sido el artículo 3.6) RIE-SCTE el encargado de definir por primera vez qué se entiende por parte usuaria, que, a los efectos que aquí interesan, sería aquella «[…] persona física o jurídica que confía en la identificación electrónica o el servicio de confianza». De este modo, pese a que tradicionalmente se ha identificado a este sujeto con cualquier persona que confía en el certificado electrónico que integra una determinada firma electrónica[734], en mi opinión, esta noción ha de tener una vocación ciertamente más amplia, englobando también aquellos supuestos en que la firma electrónica que pretende generar confianza no goza de dicho certificado (por ejemplo, firma electrónica simple). Además, si bien es cierto que, en el caso que nos ocupa, el tercero que confía es analizado desde la óptica de la concreta relación negocial determinante del contrato electrónico, podría abarcar a cualquier persona que confíe o tenga interés en confiar en la autenticidad de una firma electrónica suscrita por el firmante[735], aun cuando esta no constituyera o determinara el nacimiento de relación contractual alguna.

Se trata, por lo demás, de una expresión procedente del sistema jurídico anglosajón, que no goza de tratamiento especializado y separado[736], si bien es cierto que la ley reconocerá ciertos efectos a los terceros que confían, como el derecho a la indemnización en los supuestos de responsabilidad del firmante cuando este asume la posición de PSSI y aquel la de DSSI. En cualquier caso, podemos decir que será este el sujeto receptor que, dentro de la firma digital, se encargue de emplear la clave pública (a través del dispositivo de verificación de firma electrónica) del firmante para descifrar el contenido del documento electrónico y volver al mensaje en claro[737].

Para concluir, y al igual que dijimos respecto del firmante, dentro de la relación contractual que se establezca, el tercero que confía podrá adquirir la condición de PSSI o la de DSSI, y, dentro de esta última, la de consumidor. En consecuencia, y dependiendo del supuesto concreto, tendremos que tener en cuenta la aplicación cumulativa de varias normativas de forma simultánea.

---

[734] MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., p. 141.

[735] VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, cit., p. 143.

[736] MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., p. 141.

[737] BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», cit., p. 412.

3. Tercero generador de confianza como sujeto activo intermediador: el problema de la descoordinación normativa

El nuevo Reglamento europeo eIDAS ha supuesto una profunda transformación en la concepción y en la misma denominación de los sujetos o entidades encargados de prestar servicios de confianza en el ámbito de las transacciones electrónicas desarrolladas en el mercado interior. En efecto, con la entrada en vigor de la nueva normativa comunitaria, se amplía el ámbito de aplicación de la actividad desempeñada por los conocidos como *PSSIisc* (antes, y por los motivos que se expondrán a continuación, *PSSIic*), *autoridades de certificación*, *entidades de certificación* o *proveedores de servicios de certificación*, que no se reduce ya, como antaño y gracias a la expansión propia de los servicios de confianza regulados, a la firma electrónica.

Así las cosas, tal y como establece el apartado 19) del artículo 3 RIE-SCTE, estos prestadores (que ya no recibirán el nombre de PSSIic, sino el más correcto de PSSIisc) vendrán personificados en aquellas personas, físicas o jurídicas, que prestan uno o más SSIisc[738]. A su vez, y dependiendo de la cualificación (o ausencia de la misma) que tengan estos SSIisc, hablaremos de PSSIisc *cualificados* o de PSSIisc *no cualificados*.

Los PSSIisc cualificados, como bien puede deducirse, serán aquellos que presten uno o varios SSIisc; no obstante, a esta exigencia se añade una adicional, y es la necesidad de que el organismo de supervisión les haya concedido la cualificación –artículo 3.20) Reglamento eIDAS– (**anexo XXVI**). Ha sido el extenso artículo 17 del Reglamento europeo el encargado de regular la designación y funciones de este órgano. De acuerdo con este precepto, el organismo de supervisión será designado por cada Estado miembro de entre los establecidos en su territorio o, previo acuerdo mutuo con otro Estado miembro, de entre los establecidos en el territorio de este último, siendo notificados sus nombres y direcciones a la Comisión. Responsables de las funciones de supervisión dentro del Estado miembro que lo designe, disfrutarán de las competencias necesarias y de los recursos adecuados; en concreto, estas funciones se reducirán a dos: una primera, consistente en supervisar a los PSSIisc cualificados que se hallen establecidos en el territorio del Estado miembro que lo designe, con el objetivo

[738] Recordemos, SSIi consistentes en: a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios; b) la creación, verificación y validación de certificados para la autenticación de sitios web, o c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios –artículo 3.16) y 17) Reglamento eIDAS–.

de garantizar, mediante actividades de supervisión previas y posteriores, que tales PSSIisc cualificados y los SSIisc cualificados que prestan cumplen los requisitos establecidos en el presente Reglamento; una segunda, centrada en adoptar, caso de que resulte necesario, medidas en relación con los PSSIisc no cualificados establecidos en el territorio del Estado miembro que lo designe, a través de actividades de supervisión posteriores y siempre que reciba la información de que dichos PSSIisc no cualificados o los SSIisc no cualificados que prestan no cumplen, supuestamente, los requisitos establecidos en el presente Reglamento (apartado tercero).

Prosigue el apartado siguiente, para el cumplimiento de las funciones anteriores, y con las limitaciones establecidas, el organismo de supervisión realizará, en particular, las siguientes actividades: a) cooperar con otros organismos y prestarles asistencia, de conformidad con el artículo 18 RIE-SCTE[739]; b) analizar los informes de evaluación de la conformidad a que se

[739] Este artículo 18 del Reglamento europeo regula la asistencia mutua entre organismos de supervisión con el fin de intercambiar prácticas idóneas. En este sentido, un organismo de supervisión, previa solicitud justificada de otro, deberá prestarle asistencia con el objetivo de que las actividades de los organismos de supervisión en su conjunto puedan realizarse de manera coherente. Esta asistencia podrá incluir, en particular, las solicitudes de información y las medidas de supervisión, tales como aquellas peticiones para que se lleven a cabo inspecciones en relación con los informes de evaluación de la conformidad a que se refieren los artículos 20 y 21 RIE-SCTE (apartado primero). Pese a lo anterior, el organismo de supervisión al que se le dirija la solicitud podrá denegarla cuando no sea competente para prestar la asistencia pedida, cuando dicha asistencia no guarde proporción con las actividades de supervisión del organismo de supervisión previstas en el artículo 17 o cuando la prestación de la ayuda fuera incompatible con el Reglamento eIDAS (apartado segundo). En cualquier caso, cuando proceda, los Estados miembros podrán autorizar a sus respectivos organismos de supervisión para que lleven a cabo investigaciones conjuntas con participación de personal de los organismos de supervisión de otros Estados miembros; los acuerdos y procedimientos para dichas actividades conjuntas serán aprobados y establecidos por los Estados miembros de que se trate de conformidad con sus legislaciones nacionales (apartado tercero).

refieren los artículos 20.1[740] y 21.1[741] RIE-SCTE; c) informar a otros organismos de supervisión y al público en general de la violación de la seguridad o la pérdida de la integridad, de

[740] De acuerdo con este precepto, los PSSIisc cualificados serán preceptivamente auditados, como mínimo, cada dos años, por un organismo de evaluación de la conformidad, asumiendo los gastos que ello genere. Este organismo aparece definido en el artículo 2.13) RRAVMRCP (DOUE L 218, de 13 de agosto de 2008, p. 30), entendiendo por tal el «[…] organismo que desempeña actividades de evaluación de la conformidad, que incluyen calibración, ensayo, certificación e inspección»; a su vez, la evaluación de la conformidad, adiciona el apartad precedente del mismo precepto, hará referencia al «[…] proceso por el que se demuestra si se cumplen los requisitos específicos relativos a un producto, un proceso, un servicio, un sistema, una persona o un organismo». La competencia de este organismo para realizar una evaluación de conformidad de un PSSIisc cualificado y de los SSIisc que presta está acreditada en virtud del RIE-SCTE –artículo 3.18) Reglamento eIDAS–. La finalidad de la auditoría será confirmar que tanto los PSSIisc cualificados como los SSIisc cualificados que prestan cumplen los requisitos establecidos en el Reglamento; obtenido el mismo, será enviado por el PSSIisc cualificado al organismo de supervisión en el plazo de tres días hábiles tras su recepción (apartado primero). Sin perjuicio de lo anterior, el organismo de supervisión podrá en cualquier momento auditar o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la conformidad de los PSSIisc cualificados, que correrán con los gastos originados, a fin de confirmar que tanto estos prestadores como los SSIisc cualificados que prestan cumplen los requisitos del RIE-SCTE; caso de infracción de las normas sobre protección de datos personales, el organismo de supervisión informará a las autoridades de protección de datos de los resultados de sus auditorías (apartado segundo). En el supuesto de que, como consecuencia de la labor de comprobación realizada, el organismo de supervisión requiera a un PSSIisc cualificado que corrija el incumplimiento de requisitos del presente Reglamento y este no actúe en consecuencia dentro del plazo fijado por dicho organismo, este, teniendo en cuenta particularmente el alcance, la duración y las consecuencias de este incumplimiento, podrá retirar (y, a tal efecto, así se lo comunicará) la cualificación al PSSIisc o al SSIisc que este presta e informar al organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales, a efectos de que se actualice la lista de confianza del artículo 22 RIE-SCTE (apartado tercero). Por lo demás, la Comisión podrá, mediante actos de ejecución (a adoptar con arreglo al procedimiento de examen contemplado en el artículo 48.2 RIE-SCTE), establecer números de referencia de las siguientes normas: a) para la acreditación de los organismos de evaluación de la conformidad y para el informe de evaluación de la conformidad; b) sobre las disposiciones en materia de auditoría con arreglo a las cuales los organismos de evaluación de la conformidad realizarán la evaluación de la conformidad de los PSSIisc cualificados (apartado cuarto). Siguiendo los términos previstos en este precepto, el artículo 11.3.e) ALSEC establece la obligación de todo PSSIisc cualificado de envía el informe de evaluación de la conformidad al Ministerio de Energía, Turismo y Agenda Digital, conllevando su incumplimiento «[…] la suspensión de la cualificación al prestador y al servicio que éste presta, y su eliminación de la lista de confianza prevista en el artículo 22 del citado Reglamento hasta que se aporte el informe de evaluación».

[741] Por su parte, el artículo 21 RIE-SCTE regula aquellos casos en que PSSIisc sin cualificación tengan la intención de iniciar su actividad como PSSIisc cualificados; en estos casos, habrán de presentar al organismo de supervisión una notificación de su intención junto con un informe de evaluación de la conformidad expedido

conformidad con el artículo 19.2 RIE-SCTE[742]; d) informar a la Comisión de sus actividades principales, de conformidad con el apartado sexto del presente precepto; e) realizar auditorías o solicitar a un organismo de evaluación de la conformidad que realice una evaluación de la

por un organismo de evaluación de la conformidad (apartado primero). Verificado en sentido afirmativo por el organismo de supervisión que el PSSIisc y los SSIisc que presta cumplen los requisitos establecidos en el Reglamento eIDAS para los PSSIisc cualificados y SSIisc cualificados, concederá la cualificación al PSSIisc y a los SSIisc que presta y lo comunicará al organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales, dentro de los tres meses desde la notificación de dicha conformidad; si la verificación no concluye en el plazo de tres meses, el organismo de evaluación informará de ello al PSSIisc, especificando los motivos de la demora y el plazo previsto para concluir la verificación (apartado segundo). Por lo demás, los PSSIisc a los que se les haya concedido la cualificación podrán comenzar a prestar el SSIisc cualificado una vez que la misma haya sido indicada en las listas de confianza del artículo 22 RIE-SCTE (apartado tercero). Por último, la Comisión podrá, mediante actos de ejecución (a adoptar con arreglo al procedimiento de examen contemplado en el artículo 48.2 RIE-SCTE), definir los formatos y procedimientos a efectos de cuanto se ha expuesto (apartado cuarto).

[742] De acuerdo con el artículo 19 del Reglamento eIDAS, los PSSIisc cualificados y los PSSIisc no cualificados adoptarán las medidas técnicas y organizativas necesarias para gestionar los riesgos para la seguridad de los SSIisc que respectivamente presten; teniendo en cuenta los avances tecnológicos, estas medidas habrán de garantizar un nivel de seguridad proporcionado al grado de riesgo. En concreto, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad e informar a los interesados de los efectos negativos de cualesquiera de los mismos (apartado primero). En cualquier caso, los PSSIisc cualificados y los PSSIisc no cualificados, sin demoras indebidas y en un máximo de un día tras tener conocimiento de ellas, notificarán al organismo de supervisión y, caso de que sea necesario, a otros organismos relevantes como el organismo nacional competente en materia de seguridad de la información o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el SSIisc prestado o en los datos personales correspondientes. Cuando dicha violación de la seguridad o pérdida de la integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el SSIisc, el PSSIisc se lo notificará también, sin demora indebida, a la persona en cuestión. Además, cuando proceda, en especial en aquellos casos en que la violación de la seguridad o la pérdida de la integridad afecte a más de un Estado miembro, el organismo de supervisión notificado informará al respecto a los organismos de supervisión de los demás Estados miembros afectados y a la ENISA. Junto a lo anterior, el organismo de supervisión informará al público o exigirá al PSSIisc que lo haga, siempre que considere que la divulgación de la violación de la seguridad o la pérdida de la integridad reviste interés público (apartado segundo). Anualmente, el organismo de supervisión facilitará a la ENISA un resumen de las notificaciones de violación de la seguridad o pérdida de la integridad recibidas por parte de los PSSIisc (apartado tercero). Por último, la Comisión, mediante actos de ejecución (a adoptar con arreglo al procedimiento de examen contemplado en el artículo 48.2 RIE-SCTE), establecerá una mayor especificación de las medidas a que se refiere el apartado primero y la definición de los formatos y procedimientos, incluidos los plazos, aplicables a efectos del apartado segundo.

conformidad de los PSSIisc cualificados, con arreglo al artículo 20.2 RIE-SCTE; f) cooperar con las autoridades de protección de datos, en particular, informándoles, sin demora indebida, de los resultados de las auditorías de los PSSIisc cualificados, en el caso de posible infracción de las normas sobre protección de datos personales; g) conceder la cualificación a los PSSIisc y a los SSIisc que presten, así como retirar esta cualificación, con arreglo a los artículos 20 y 21 RIE-SCTE; h) comunicar al organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales de su decisión de conceder o retirar la cualificación, salvo en el caso en el que dicho organismo sea también el organismo de supervisión[743]; i ) verificar la existencia y la correcta aplicación de las disposiciones relativas

[743] Por lo que respecta a las listas de confianza, estas se encuentran, como decíamos, reguladas en el artículo 22 RIE-SCTE, que establece la obligación de todo Estado miembro de establecer, mantener y publicar de manera segura dichas listas, listas que contendrán información relativa a los PSSIisc cualificados de los que el Estado miembro en cuestión sea responsable, junto con la información relacionada con los SSIisc cualificados que aquellos presten (apartado primero). Estas listas de confianza deberán ir firmadas o selladas electrónicamente en una forma apropiada para el tratamiento automático, no estableciéndose la modalidad concreta de firma o sello electrónico que preceptivamente halla de incorporar (apartado segundo). Los Estados miembros deberán notificar a la Comisión, sin retrasos indebidos (aunque no se establece un plazo concreto), información sobre el organismo responsable del establecimiento, mantenimiento y publicación de las listas de confianza nacionales, así como detalles relativos al lugar en que se publiquen dichas listas, los certificados empleados para firmar o sellar las listas de confianza (lo que indica que la firma o sello electrónico habrá de ser, como mínimo, avanzado o cualificado) y cualquier modificación de los mismos (apartado tercero). A continuación, la Comisión pondrá a disposición del público, por medio de un canal seguro, la información a que se refiere el apartado anterior, en una forma firmada o sellada electrónicamente y apropiada para el tratamiento automático (apartado cuarto). Por último, se establecía como fecha máxima el 18 de septiembre de 2015 para que la Comisión, mediante actos de ejecución (a adoptar con arreglo al procedimiento de examen contemplado en el artículo 48.2 RIE-SCTE), especificara la información a que se refiere el apartado primero y definiera las especificaciones técnicas y los formatos de las listas de confianza, aplicables a efectos de los apartados primero a cuarto (apartado quinto); fruto de esta previsión, surge la DEETFLC. Por lo demás, dispone el artículo 23 RIE-SCTE, una vez que la cualificación a que se refiere el artículo 21.2.2º Reglamento eIDAS se haya incluido en la lista de confianza a que nos referíamos, los PSSIisc cualificados podrán usar la etiqueta de confianza «UE» para indicar de manera simple, reconocible y clara los SSIisc cualificados que prestan (apartado primero). Al usar esta etiqueta, los PSSIisc cualificados garantizarán que en su sitio web existe un enlace a la lista de confianza en cuestión (apartado segundo). Finalmente, como muy tarde el 1 de julio de 2015, la Comisión, por medio de actos de ejecución (a adoptar con arreglo al procedimiento de examen contemplado en el artículo 48.2 RIE-SCTE), elaborará especificaciones relativas a la forma y, en particular, la presentación, composición, tamaño y diseño de la etiqueta de confianza «UE» para SSIisc cualificados (apartado tercero); como resultado de esta previsión, nace el REER-FECUESCC.

a los planes de cese, en el caso de que los PSSIisc cesen sus actividades, con inclusión de la forma en que se hace accesible la información, con arreglo al artículo 24.2.h) RIE-SCTE, y j) requerir que los PSSIisc corrijan cualquier incumplimiento de los requisitos establecidos en el presente Reglamento.

Asimismo, los Estados miembros podrán disponer que el organismo de supervisión establezca, mantenga y actualice una infraestructura de confianza, de conformidad con las condiciones que establezca la legislación nacional (artículo 17.5 Reglamento eIDAS). Obligación de este organismo será también la de presentar a la Comisión y la de poner a disposición de los Estados miembros, el 31 de marzo de cada año, un informe sobre sus actividades principales del año civil precedente, junto con un resumen de las notificaciones de violación recibidas de los PSSIisc, de acuerdo al artículo 19.2 RIE-SCTE (apartados 5 y 6 del artículo 17 Reglamento eIDAS)[744].

Con anterioridad al Reglamento eIDAS, sin embargo, la opción comunitaria se inclinaba por el término *proveedor*[745], definiéndolo como «[…] la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica» –artículo 2.11) DFE–. De esta definición (en concreto, de la conjunción *o*) podemos extraer como conclusión que la actividad de expedición de certificados del, por entonces, PSSIic, no tenía por qué darse obligatoriamente, sino que cabía la posibilidad de que dicho prestador fuera considerado como tal por «[…] prestar otros servicios en relación con la firma electrónica»; ello determinaba, en mi opinión, la incorreción del término empleado para definir a tales sujetos, conclusión que hubiera sido la misma aun cuando la conjunción *o* hubiera sido sustituida por la conjunción *y* y, por tanto, la actividad de certificación fuera necesaria, ya que, en cualquier caso, no hubiera sido exclusiva, habiendo de encontrar un término que consiguiera abarcar la totalidad de funciones desarrolladas por dichos prestadores. Por lo demás, la DFE no distingue, dentro del elenco de definiciones del artículo segundo, entre PSSIic

[744] La Comisión podrá, mediante actos de ejecución (a adoptar con arreglo al procedimiento de examen contemplado en el artículo 48.2 RIE-SCTE), definir los formatos y procedimientos relativos al informe a que se refiere el apartado 6 (artículo 17.8 Reglamento eIDAS).

[745] En opinión de autores como MARTÍNEZ NADAL, A., «Firma electrónica», cit., p. 175, ello «[…] pone de manifiesto una voluntad de evitar siquiera la apariencia de atribución de naturaleza pública que sí podrían sugerir otras denominaciones (p. ej., autoridad de certificación), y posibilitando así su naturaleza estrictamente comercial».

*reconocidos* (sinónimo de los que ahora se conocen como *cualificados*) y PSSIic *no reconocidos*, si bien es cierto que, en ciertos preceptos como el sexto, sí que parece deducirse esta distinción.

Lo mismo sucede en nuestro ordenamiento jurídico interno con la LFE, cuyo artículo 2.2 denomina prestador (no ya proveedor, si bien ambos términos vienen a actuar como sinónimos) de servicios de certificación a la persona, física o jurídica, que expide certificados *o* presta otros servicios en relación con la firma electrónica; de nuevo, se incurre en el mismo error de denominación apuntado al hablar de la DFE. A ello se añadirá el más importante del ámbito de aplicación, que no se ceñirá ya únicamente a la firma electrónica, sino que comprenderá también otros servicios de confianza. En consecuencia, hasta tanto no sea modificada o derogada esta Ley, habrá de entender sustituido el término PSSIic por el de PSSIisc y considerar ampliado el ámbito de aplicación a aquel que establece el artículo 3.16) RIESCTE. Por lo demás, tampoco aquí se distinguirá claramente entre PSSIic *reconocidos* y PSSIic *no reconocidos*, aludiéndose a aquellos en modo indirecto como *PSSIic que expidan certificados reconocidos* (véase, entre otros, el artículo 20.1 LFE), afirmación esta inexacta en tanto que, a tenor de la definición *supra* expuesta, la norma tendría que aludir a los mismos como *PSSIic que expidan certificados reconocidos o presten otros servicios reconocidos en relación con la firma electrónica.*

Más correcta era, pese a no coincidir exactamente con la de la DFE a la que pretendía adecuarse, la definición de PSSIic contenida en el artículo 2.k) RDLFE. Así es, de acuerdo con la misma, esta figura vendrá representada por «[…] la persona física o jurídica que expide certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica[746]»[747]. Con esta redacción, se eliminaba el problema anterior, exigiendo que el PSSIic desempeñara, como mínimo, tareas de certificación (de ahí su propia denominación, ahora

[746] Como bien señala, al referirse al RDLFE, *Ibid.*, p. 176, «[…] tales servicios pueden ser inherentes al propio certificado y necesarios (revocación y suspensión en caso de pérdida de la clave privada u otro elemento de firma, servicio al que se refieren los arts. 11 *e*, 12 *c*, además del art. 9), otros más bien discutibles (generación de las claves, permitida al prestador tanto en el ordenamiento comunitario como en el español, y, en particular, copia o almacenamiento de las mismas, actividad esta última respecto de la que […] existen diferencias entre ambos ordenamientos), así como otros complementarios pero igualmente necesarios para la seguridad del sistema de certificados en particular o del comercio electrónico en general (por ejemplo, de forma respectiva, servicio de sellado temporal, previsto siquiera de forma parcial en el art. 12 *a* o actuación como notario electrónico)».

[747] En la misma línea, el artículo 2.e) LMFE, que por PSSIic entiende «[…] la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas».

sí, del todo correcta), mínimo que *podría* verse acompañado de otros servicios en relación con la firma electrónica.

En cualquier caso, el PSSIisc se erige en un elemento fundamental dentro del sistema de firma electrónica, al conferir la seguridad jurídica necesaria a aquellas comunicaciones realizadas por medios telemáticos y encaminadas a la perfección de un contrato vía electrónica, dando origen a la mayoría de las normas específicas existentes sobre esta materia[748]. Para dar continuidad a esta importante figura ante el cambio de norma, el artículo 51.3 RIE-SCTE dispone que aquel PSSIisc que emitiese certificados reconocidos conforme a la DFE habrá de presentar un informe de evaluación de la conformidad al organismo supervisor lo antes posible, si bien, como máximo, el 1 de julio de 2017; hasta tanto esta exigencia tenga lugar, es decir, hasta que el PSSIic en cuestión presente el citado informe y el organismo supervisor ultime su análisis (no basta, pues, con presentarlo), dicho prestador será considerado, según el Reglamento eIDAS, como PSSIisc cualificado. Consecuencia de lo anterior, de no presentar el informe en plazo, tal PSSIic no podrá ser considerado, a los efectos del RIE-SCTE, como PSSIisc cualificado a partir del día siguiente, el 2 de julio de 2017 (artículo 51.3 del Reglamento europeo).

### 3.1. Ámbito de aplicación y principios rectores de la actividad

Para garantizar el cumplimiento de los objetivos establecidos en la normativa en materia de contratación y firma electrónicas, el legislador opta por superar las diferencias legislativas existentes entre los Estados miembros y establece el principio en virtud del cual todos ellos reconocerán la legislación interna de los demás, pese a las diferencias existentes con la suya propia (principio de reconocimiento mutuo o de libre prestación de SSI); así, cuando un SSI sea prestado desde un Estado miembro a un DSSI situado en otro Estado miembro, este último se abstendrá de intervenir en dicha relación, relación que se regirá en todos sus aspectos por la ley del país en el que esté establecido el PSSI (principio de aplicación de la ley del país de origen)[749]. Sendos principios encuentran cobijo legal general en el artículo 3 DCE,

[748] MADRID PARRA, A., «Seguridad en el comercio electrónico», cit., pp. 138 y 139.

[749] DÍAZ FRAILE, J. M., «El comercio electrónico: Directiva y Proyecto de ley español de 2000. Crónica de su contenido, origen, propósitos y proceso de elaboración», *Actualidad civil*, vol. 1, 2001, p. 49. El considerando 22 DCE precisa el fundamento de esta regla, al establecer que el control de los SSI debe hacerse en el origen de la actividad para garantizar que se protegen de manera eficaz los intereses generales. Así, a fin de proteger la libre circulación de SSI y la seguridad jurídica de quienes los prestan y de quienes los reciben, en principio, estos SSI

que comienza con una taxativa enunciación del principio de aplicación de la ley del país de origen: todo Estado miembro velará por que los SSI facilitados por un PSSI establecido en su territorio respeten el conjunto de disposiciones nacionales aplicables en el territorio de dicho Estado miembro que formen parte del ámbito normativo coordinado. Lo propio hace el apartado segundo con el principio de reconocimiento mutuo o de libre prestación de SSI: los Estados miembros no podrán restringir la libertad de prestación de SSI de otro Estado miembro por razones inherentes al ámbito normativo coordinado[750]. De este modo, ambos principios se complementan de la siguiente manera: los Estados no podrán oponer las normas del país de acogida del servicio (normas del país de residencia del DSSI), incluso si dicho SSI transfronterizo no cumple con los requisitos impuestos para este mismo ámbito normativo coordinado por las normas del Estado de acogida, con los límites del orden público y de las normas imperativas[751].

A estos principios, centrados en la aplicación de la norma, se añade un tercero, específico del sujeto encargado de prestar el servicio: el PSSI. Estamos hablando del principio de no sujeción a autorización previa, tradicional en nuestro sistema normativo nacional y comunitario y que, como veremos seguidamente, experimenta una nueva visión como consecuencia de la entrada en vigor del nuevo Reglamento europeo eIDAS.

---

deben estar sujetos al régimen jurídico del Estado miembro en que esté establecido el PSSI, siendo indispensable delimitar con precisión los contornos de la responsabilidad de dicho Estado miembro para poder mejorar la confianza mutua entre todos ellos; para ello, añade, será necesario «[…] que la autoridad competente garantice dicha protección no sólo en el caso de los ciudadanos de su país, sino en el de todos los ciudadanos de la Comunidad».

[750] Sobre esta cuestión, *vid.* CALVO CARAVACA, A. Y OTROS, *Conflictos de leyes y conflictos de jurisdicción en Internet*, cit., pp. 34 y 35; CLARIZIA, R., *I contratti informatici*, cit., p. 37; GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, cit., pp. 232 y 233; PEGUERA POCH, M. Y OTROS, «Marco jurídico de los servicios de la sociedad de la información y del comercio electrónico», cit., pp. 327 a 329; XALABARDER PLANTADA, R., «La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios», *Revista de Internet, Derecho y Política*, vol. 2, 2006, pp. 14 y 14.

[751] VARGAS GÓMEZ-URRUTIA, M., «Protección internacional de los consumidores, contratos y comercio electrónico», en BOTANA GARCÍA, G. A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 660 a 664.

### 3.1.1. Principio de aplicación de la ley del país de origen

Cuando la actividad económica en que consiste la prestación de un SSI se lleve a cabo a través de una instalación estable y por un período de tiempo indefinido, diremos que estamos ante un PSSI *establecido*, definido en la letra c) del artículo 2 DCE[752]; ahora bien, aclara a continuación el precepto, «[…] la presencia y utilización de los medios técnicos y de las tecnologías utilizadas para prestar el servicio no constituyen en sí mismos el establecimiento del prestador de servicios», ya que la complejidad de Internet como espacio de comunicación trae consigo que, en ocasiones, un PSSI establecido en un Estado tenga que utilizar medios tecnológicos sitos físicamente en otro, sin que ello suponga considerarle establecido en este último país[753]. Así, añade el considerando 19 DCE, cuando se trate de una sociedad que proporcione SSI mediante un sitio en la Red, el lugar de establecimiento del PSSI no se encontrará allí donde esté la tecnología que mantiene el sitio web ni allí donde se pueda acceder al mismo, sino en el lugar en el que se desarrolle la actividad económica propiamente dicha. En el supuesto de que existan varios establecimientos de un mismo PSSI, aclara, es importante determinar desde qué lugar de establecimiento se presta un SSI concreto; en caso de especial dificultad para determinar a partir de cuál de los lugares de establecimiento se presta un SSI dado, este será aquel en el que el PSSI tenga su centro de actividades en relación con ese SSI en particular.

Por su parte, de la noción de *establecimiento* se ocupa, a nivel internacional, el artículo 4.h) CNUUCECI, en virtud del cual se entenderá por tal «[…] todo lugar donde una parte mantiene un centro de operaciones no temporal para realizar una actividad económica distinta del suministro transitorio de bienes o servicios desde determinado lugar». En España, es el párrafo segundo del apartado II de la Exposición de Motivos de la LSSICE el que proporciona una definición de establecimiento como «[…] el lugar desde el que se dirige y gestiona

[752] Como bien ha señalado el considerando 19 DCE, este requisito se cumple también cuando se constituye una sociedad durante un período determinado. Por lo demás, y como bien apunta PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, cit., pp. 54 y 55, a diferencia de la DCE, no se contiene en la LSSICE una definición de PSSI establecido, si bien se ocupa de esta figura en su artículo segundo.

[753] ARIAS POU, M., *Manual práctico de comercio electrónico*, cit., p. 70.

una actividad económica», definición que completa al incluir que «[…] se inspira en el concepto de domicilio fiscal recogido en las normas tributarias españolas y que resulta compatible con la noción material de establecimiento predicada por el Derecho comunitario».

De la conjunción de todo lo anterior, podemos concluir que, dentro de nuestro ordenamiento jurídico interno, el lugar de establecimiento del PSSI ejerce una triple finalidad: en primer lugar, dispone el ámbito de aplicación de la normativa en materia de contratación y firma electrónicas; en segundo lugar, determina también la aplicación adicional de todas las demás disposiciones del ordenamiento jurídico español que les resulten de aplicación en función de la actividad específicamente desarrollada, y, en tercer lugar, precisa la ley y las autoridades encargadas del control de su cumplimiento, de acuerdo con el principio de la aplicación de la Ley del país de origen que inspira la DCE y, consecuentemente, la LSSICE.

Partiendo de las premisas anteriores, y sobre la base del artículo 3.1 DCE, la LSSICE (de forma principal global para todos los PSSI) y la LFE/ALSEC (de forma accesoria y específica para los PSSIisc) dedican el Capítulo II del Título I (artículos 2 a 4) y el artículo 2, respectivamente, a regular el ámbito de aplicación de quienes prestan SSIisc. De este grupo de preceptos podemos distinguir tres supuestos de hecho posibles: a) PSSI establecidos en España (y, dentro de estos, PSSI que cuentan con un establecimiento permanente situado en nuestro país), b) PSSI establecidos en otro Estado miembro de la UE o del EEE y, por último, c) PSSI establecidos en un Estado no perteneciente a la UE o al EEE (**anexo XXVII**).

Por lo que respecta al primero de los grupos indicados, sostiene el artículo 2.1 LSSICE (precedido por el más escueto artículo 1.1 RDLFE) que esta Ley será de aplicación, en cualquier caso, a aquellos *PSSI que estén establecidos en España (sean, o no, españoles) y a los SSI por ellos prestados* (con independencia de que todos, o tan sólo parte de ellos, se presten en nuestro país). Como decíamos anteriormente, el concepto de establecimiento se inspira en el concepto de domicilio fiscal contenido en las normas tributarias españolas, más específicamente en la LGTr[754], que, en su artículo 48.1, define el domicilio fiscal como «[…] el lugar de localización del obligado tributario en sus relaciones con la Administración tributaria»[755]. Pues

[754] BOE núm. 302, de 18 de diciembre de 2003.

[755] De acuerdo con esta definición, el precepto establece el domicilio fiscal atendiendo a la siguiente clasificación: a) para las personas físicas, el lugar donde estas tengan su residencia habitual, si bien, en el caso de que desarrollen principalmente actividades económicas en los términos que reglamentariamente se determinen, la

bien, partiendo de esta previsión normativa, la LSSICE (artículo 2.1) dispone que se considerará que un PSSI está establecido en nuestro país cuando su residencia (personas físicas) o su domicilio social (personas jurídicas) se encuentre en territorio español y siempre que esta ubicación coincida con el lugar en el que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios; de no cumplirse este último supuesto, se atenderá al lugar en el que se realice dicha gestión o dirección[756].

---

Administración tributaria podrá considerar como domicilio fiscal el lugar en el que esté efectivamente centralizada la gestión administrativa y la dirección de las actividades por ellas desarrolladas, prevaleciendo, de no poder establecerse dicho lugar, aquel donde radique el mayor valor del inmovilizado en el que se realicen dichas actividades económicas –apartado a) del artículo 48.2 LGTr–; b) para las personas jurídicas, su domicilio social, siempre y cuando en él esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios, ya que, de lo contrario, se tomará en consideración el lugar en el que se lleve a cabo dicha gestión o dirección, adquiriendo preeminencia, cuando no pueda determinarse el domicilio fiscal atendiendo a los criterios anteriores (al igual que en el supuesto de personas físicas), el lugar donde radique el mayor valor del inmovilizado –apartado b) del artículo 48.2 LGTr–; c) para las herencias yacentes, las comunidades de bienes y las demás entidades que, carentes de personalidad jurídica, constituyan una unidad económica o un patrimonio separado susceptible de imposición (artículo 35.4 LGTr), regirán los mismos criterios para determinar el domicilio fiscal que los previstos para las personas jurídicas –apartado c) del artículo 48.2 LGTr–, y, por último, para las personas o entidades no residentes en España, el domicilio fiscal se determinará atendiendo a la normativa reguladora de cada tributo –apartado d) del artículo 48.2 LGTr–. Como regla supletoria, se prevé la aplicación del domicilio del representante que los obligados tributarios que no residan en España deben designar como domicilio en territorio español (artículo 47 LGTr), bien cuando operen en nuestro territorio a través de un establecimiento permanente, bien cuando lo establezca expresamente la normativa tributaria, bien cuando, dadas las características de la operación o de la actividad realizada o por la cuantía de la renta obtenida, así lo requiera la Administración tributaria; no obstante, cuando la persona o entidad no residente en España opere mediante un establecimiento permanente, el domicilio fiscal será el que resulte de aplicar a dicho establecimiento permanente las reglas establecidas para las personas físicas y para las personas jurídicas –artículo 48.2, *in fine*, LGTr–.

[756] Este supuesto, que guarda un cierto paralelismo con la regla general contenida en el artículo 15.4.a) LMCE, sostiene, en su apartado final que la normativa española será aplicable al PSSI de que se trate y a los SSI que preste por la sencilla razón de que es en nuestro país donde tiene efectivamente centralizada la gestión administrativa y la dirección de sus negocios, más allá de que tenga (o no) su residencia (si el PSSI es persona física) o su domicilio social (si el PSSI es persona jurídica) en otro Estado que no sea España. De todo ello se desprenden tres posibilidades: a) que la residencia o el domicilio social del PSSI y el lugar en el que está efectivamente centralizada la gestión administrativa y la dirección de sus negocios se encuentren en España, en cuyo caso se considerará que dicho PSSI se encuentra establecido en territorio español, siéndole aplicable, por tanto, la LSSICE y todas las demás disposiciones del ordenamiento jurídico relacionadas con su ámbito de actividad, independientemente de la utilización (o no) de medios electrónicos para su realización; b) que la residencia o el

Además de aplicarse a los PSSI establecidos en España, la norma también estará dirigida a los *SSI que PSSI residentes (personas físicas) o domiciliados (personas jurídicas) en otro Estado (sea este un Estado miembro o no) ofrezcan a través de un establecimiento permanente situado en España* (artículo 2.2 LSSICE, precepto este que no encuentra referencia alguna en la DCE); en este supuesto, como podemos observar, la sujeción es parcial, pues únicamente afecta a los SSI que, de manera efectiva, se presten en territorio nacional. A tal efecto, se presumirá que un PSSI actúa a través de un establecimiento permanente situado en nuestro país cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda (en cuyo caso será de aplicación la LSSICE a todos los SSI que preste el PSSI, ya que todos ellos son prestados desde el establecimiento permanente situado en España) o parte de su actividad (siendo aquí aplicable la LSSICE tan sólo respecto de aquellos SSI que el PSSI preste mediante un establecimiento permanente situado en España).

El artículo 2.3 LSSICE contiene, por su parte, una presunción de establecimiento en virtud de la cual se entenderá que el PSSI está establecido en España cuando él o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en cualquier otro registro público español en el que se exigiera esta inscripción para la adquisición de personalidad jurídica[757]. En cualquier caso, continúa este mismo precepto inspirándose claramente en el artículo 2.c), *in fine*, DCE, el empleo de medios tecnológicos que se encuentren situados en territorio español

---

domicilio social del PSSI se encuentre en España y el lugar en el que está efectivamente centralizada la gestión administrativa y la dirección de sus negocios se encuentren en otro Estado distinto a España, en cuyo caso no será de aplicación ni la LSSICE ni ninguna de las demás disposiciones del ordenamiento jurídico afectadas, y c) que la residencia o el domicilio social del PSSI se encuentre en un país que no sea España y el lugar en el que está efectivamente centralizada la gestión administrativa y la dirección de sus negocios se encuentren en España, en cuyo caso se considerará que dicho PSSI se encuentra establecido en territorio español, siéndole aplicable, por tanto, la LSSICE y todas las demás disposiciones del ordenamiento jurídico relacionadas con su ámbito de actividad, más allá de la utilización (o no) de medios electrónicos para su realización.

[757] En cuanto a la determinación de los registros públicos afectados, GARCÍA MÁS, F. J., «Algunos aspectos de la ley de servicios de la sociedad de la información: el comercio electrónico, un reto de presente y de futuro. Especial consideración de la contratación electrónica», *Revista jurídica del notariado*, vol. 55, 2005, p. 77, explica cómo en algún momento de las discusiones del Borrador se discutió acerca de los Registros que deberían tenerse en cuenta para establecer esta presunción, estimando conveniente circunscribirlos a aquellos en los que la inscripción fuese necesaria para la adquisición de personalidad jurídica. Bien es cierto, en cualquier caso, que el eje pivota en torno al Registro Mercantil, donde los PSSI adoptan la forma societaria normalmente de una sociedad anónima o de una sociedad de responsabilidad limitada.

y que sirvan para la prestación o el acceso al SSI no servirá, por sí solo, como criterio para determinar el establecimiento en España del PSSI.

Para concluir, el artículo 2 concluye con un apartado cuarto en el que deja patente una obviedad, bien es cierto que necesaria o conveniente. De acuerdo con la misma, los PSSI establecidos en España estarán sujetos no sólo a esta norma, sino también a las demás disposiciones (como las provenientes de la normativa en materia de firma electrónica) que, integrantes del ordenamiento español, sean de aplicación en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

Fácil será, por ende, inferir que los PSSIisc, como modalidad singular de aquella más general de PSSI, se verán afectados íntegramente por cuanto se ha dicho anteriormente, algo que viene corroborado por el artículo 2 LFE, que, en la actualidad y hasta tanto no se derogue la norma, reproduce casi literalmente el artículo 2 LSSICE; lo mismo sucedería con el artículo 2 ALSEC, caso de entrar finalmente en vigor, pues, redactado sobre la base del artículo 2.1 RIE-SCTE[758], mantiene la misma redacción. Consecuencia de lo anterior, se verán afectados por, de manera nuclear, la LSSICE y la LFE, todos los PSSIisc establecidos en España y todos los SSIisc prestados por ellos, así como los SSIisc que, provenientes de PSSIisc residentes o domiciliados en otro Estado distinto de España, sean ofrecidos a través de un establecimiento permanente situado en nuestro país; y ello en una suerte de redacción que, actualizada y acorde con el nuevo Reglamento eIDAS, podría quedar como sigue:

> *1. La normativa en materia de servicios de la sociedad de la información y de comercio electrónico, de una parte, y de identificación electrónica y de servicios de confianza para las transacciones electrónicas, de otra, será de aplicación a los prestadores de servicios de confianza establecidos en España y a los servicios prestados por ellos.*
>
> *Se entenderá que un prestador de servicios de confianza está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios; de lo contrario, se atenderá al lugar en que se realice dicha gestión o dirección.*

[758] Apartado que, de forma positiva, delimita el ámbito de aplicación del RIE-SCTE en los siguientes términos: «[e]l presente Reglamento se aplica a los sistemas de identificación electrónica notificados por los Estados miembros *y a los prestadores de servicios de confianza establecidos en la Unión*» (la cursiva es propia).

*2. Asimismo, esta normativa será de aplicación a los servicios de confianza que los prestadores de servicios de confianza residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.*

*Se considerará que un prestador de servicios de confianza opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.*

*3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios de confianza está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.*

*La utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio de confianza no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador de servicios de confianza.*

*4. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.*

En lo atinente al segundo grupo, dispone el artículo 3.1 LSSICE (que parte, a su vez, del artículo 3.3 DCE) que, sin perjuicio de cuanto disponen los artículos 7.1 y 8 de la misma Ley, el ámbito de aplicación de la normativa española (LSSICE y demás normas que regulen la materia en cuestión –artículo 3.3 LSSICE–) alcanzará también a aquellos *PSSI establecidos en otro Estado miembro de la UE o del EEE distintos a España*, siempre que se vean satisfechas dos condiciones previas esenciales: de un lado, que presten sus SSI a DSSI radicados en España; de otro, que dichos SSI afecten a alguna de las siguientes materias: a) derechos de propiedad intelectual o industrial, b) emisión de publicidad por instituciones de inversión colectiva; c) actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios; d) obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores; e) régimen de elección por las partes contratantes de la legislación aplicable a su contrato, y f) licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas[759].

[759] No dice la LSSICE si la sujeción a la normativa española en estos casos es parcial o total, si bien entiendo que se inclina por la primera opción, dado que tiene más lógica una aplicación limitada o circunscrita tan sólo

En cualquier caso, todas las cuestiones relativas a la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se someterán a los requisitos formales de validez y eficacia establecidos en nuestro ordenamiento jurídico interno (artículo 3.2 LSSICE)[760]. Sin embargo, no será aplicable todo lo dispuesto anteriormente a aquellos supuestos en los que, de acuerdo con las normas que regulan las materias *supra* enumeradas, no fuera aplicable la ley del país en el que resida (si es persona física) o esté domiciliado[761] (si es persona jurídica) el DSSI.

No será aplicable lo dispuesto en este artículo 3 LSSICE a aquellos supuestos en que, de conformidad con las propias normas reguladoras de dichas materias, la ley del país de residencia (es decir, del establecimiento del DSSI) no fuera de aplicación (artículo 3.4 LSSICE).

Nada dice la LFE respecto de los PSSIisc establecidos en un Estado miembro de la UE o del EEE, tampoco el nuevo ALSEC. No obstante, habida cuenta de que, como ya hemos hecho constar, la DCE y la LSSICE regulan la cuestión del ámbito de aplicación normativa de forma general para todos los PSSI, ha de entenderse aplicable, por lógica, a quienes de ellos forma parte como intermediarios: los PSSIisc.

El último regula la posible aplicación de la normativa en materia de servicios de la sociedad de la información y de comercio electrónico (artículo 4 LSSICE, aspecto no contemplado en la DCE) a *PSSI establecidos, no ya fuera de nuestro país, sino también de la UE o EEE*. Para supuestos en los que la actividad de tales PSSI no está centrada de manera específica en España, señala el precepto que les será de aplicación cuanto establecen los artículos 7.2 (sometimiento a los

---

a aquellos SSI que se presten a DSSI radicados en España y que afecten, tan sólo, a alguna de las materias enumeradas.

[760] La razón estriba, sostiene PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, cit., p. 63, en que la normativa de comercio y contratación electrónicos de origen comunitario no ha podido obviar la existencia de múltiples sistemas de transmisión de bienes inmuebles, constancia esta que impidió, incluso, obtener un régimen uniforme de perfección del contrato electrónico, «[…] ya que dicha armonización quedaría ensombrecida precisamente por la diferente eficacia real que dicha norma tendría en los distintos Estados miembros». A ello responde también, entiendo, la previsión contenida en el artículo 9.2.a) DCE.

[761] La LSSICE emplea aquí, a mi juicio de manera errónea o inadecuada, el término *establecido* para referirse únicamente a personas jurídicas, cuando, como hemos visto, el mismo puede ser empleado también para las personas físicas.

acuerdos internacionales que resulten de aplicación) y 11.2 (colaboración de PSSIi establecidos en España para garantizar la efectividad de la resolución que acuerde la interrupción de la prestación de un SSI o la retirada de contenidos provenientes de un PSSI establecido en un Estado no perteneciente a la UE o al EEE) de la norma. Para aquellos otros casos de focalización específica en territorio español, la sujeción de estos concretos PSSI será más completa, ya que se verán sometidos, además, a las obligaciones previstas en la LSSICE, siempre y cuando ello no entre en conflicto con lo previsto en tratados o convenios internacionales que resulten de aplicación[762].

Tampoco se pronuncia al respecto ni la LFE ni, para el caso en que entrara en vigor, el ALSEC, si bien, al igual que decíamos respecto del supuesto anterior, tendremos que considerar aplicable todo cuanto se indica en la DCE y en la LSSICE también a los PSSIisc.

[762] Como bien apunta DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., pp. 250 y 251, la inseguridad jurídica en estos casos tendría lugar cuando la relación se produce con un PSSI que no se encuentra establecido en España ni en un Estado miembro de la UE o del EEE, ni tampoco es aplicable, caso de existir, acuerdo internacional alguno ratificado por nuestro país con el del territorio en el que dicho PSSI está establecido. Este supuesto, señala el autor, se encuentra aún sin resolver y no parece que pueda tener una fácil solución, habida cuenta de que, repetimos, dada la volatilidad del medio virtual y la falta de concreción y seguridad sobre el territorio en que se encuentra establecido un PSSI, «[…] puede producirse la circunstancia de que se esté realizando una determinada operación comercial con una persona o entidad que no se encuentre sometida a una normativa específica o que lo esté en un ámbito jurisdiccional o competencial ajeno, distante o distinto al que protege esta normativa, con lo que se produce indefectiblemente la inseguridad que citamos». La solución a estos problemas, concluye, ha de venir de la mano del DSSI, que deberá asegurarse de estar contratando con la persona adecuada y de estar cumpliéndose las garantías que acompañan a la operación desde la óptica de la normativa aplicable, competencia y jurisdicción que presenta la transacción, de acuerdo con las características de territorialidad que delimitan la aplicación de la LSSICE. También está, entiendo, la opción con que cuenta un Estado miembro, recogida por el Tribunal de Justicia, de adoptar medidas contra un PSSI establecido en otro Estado miembro (no contemplaría, pues, los casos en que el PSSI esté establecido fuera del ámbito de la UE o del EEE) cuya actividad se dirige principalmente o en su totalidad hacia el territorio del primero de los Estados, siempre que dicho establecimiento se haya realizado con la intención de evadir la legislación que resultaría aplicable dicho PSSI en caso de que se hubiera establecido en el territorio del primer Estado –considerando 57 DCE–.

### 3.1.2. Principio de reconocimiento mutuo o de libre prestación de servicios de la sociedad de la información

Por su parte, el principio de reconocimiento mutuo o de libre prestación de SSI encuentra cobijo legal general en el ordenamiento jurídico español en los artículos 7 y 8 LSSICE y 5.1 LFE. El primero de ellos, partiendo del artículo 3.2 DCE, establece que, en nuestro país, la prestación de SSI que procedan de un PSSI que se encuentre establecido en algún Estado miembro de la UE o del EEE se realizará en régimen de libre prestación de servicios, no pudiendo imponerse ningún tipo de restricción a los mismos por razones derivadas del ámbito normativo coordinado, excepto en los supuestos previstos en los artículos 3 y 8 (artículo 7.1 LSSICE)[763]; en cambio, para la aplicación de este principio a PSSI establecidos en Estados no miembros del EEE (o de la UE, se entiende), se estará a lo que se disponga en los acuerdos internacionales que resulten de aplicación (artículo 7.2 LSSICE)[764].

No obstante lo anterior, incorpora el artículo 8 LSSICE una serie de restricciones a este principio general que encuentran su fundamento original en el artículo 3.4 DCE. De acuerdo con este último precepto[765], los Estados miembros cuentan con la posibilidad de tomar medidas excepcionales dirigidas a restringir dicho reconocimiento mutuo o libre prestación de SSI entre Estados miembros, siempre que concurran cumulativamente una serie de condiciones que pasamos a desarrollar brevemente:

---

[763] Así lo anticipa el párrafo final del apartado II de la Exposición de Motivos de la LSSICE: «[…] sólo se permite restringir la libre prestación en España de servicios de la sociedad de la información procedentes de otros países pertenecientes al Espacio Económico Europeo en los supuestos previstos en la Directiva 2000/31/CE, que consisten en la producción de un daño o peligro graves contra ciertos valores fundamentales como el orden público, la salud pública o la protección de los menores. Igualmente, podrá restringirse la prestación de servicios provenientes de dichos Estados cuando afecten a alguna de las materias excluidas del principio de país de origen, que la Ley concreta en su artículo 3, y se incumplan las disposiciones de la normativa española que, en su caso, resulte aplicable a las mismas».

[764] A la vista de la previsión contenida en el artículo 7.2 LSSICE, entendemos que las restricciones previstas en el precepto octavo de la norma afectarán a PSSI establecidos en España (artículos 8.1 y 2 LSSICE) o algún Estado miembro de la UE o del EEE distinto a España (artículos 8.3 y 8.4 y 3 LSSICE), no sucediendo lo mismo con PSSI establecidos fuera de estas fronteras, que se regirán por lo dispuesto en los acuerdos internacionales que resulten de aplicación (artículo 4 LSSICE).

[765] Precedido por los considerandos 24 y 25 de la misma Directiva.

En primer lugar –artículo 3.4.a) DCE–, las medidas deberán cumplir tres exigencias fundamentales: han de ser necesarias, teniendo la consideración de tales aquellas que se fundamenten en cuestiones de orden público (en particular, las que tengan por objeto la prevención, investigación, descubrimiento y procesamiento del delito, incluidas la protección de menores y la lucha contra la instigación al odio por motivos de raza, sexo, religión o nacionalidad, así como las violaciones de la dignidad humana de personas individuales), en la protección de la salud pública, en cuestiones de seguridad pública (incluidas la salvaguarda de la seguridad y la defensa nacionales) y en la protección de los consumidores (donde se encuadran también los inversores)[766]; han de ser tomadas contra un SSI que vaya en detrimento de los de los objetivos enumerados en el inciso anterior o que presente un riesgo serio y grave de ir en detrimento de dichos objetivos y, por último, han de ser proporcionadas a tales objetivos[767]. A las anteriores se añade una posible alternativa jurídica habilitante, ya mencionada en líneas anteriores: sería aquella, defendida por el Tribunal de Justicia, que permite a un Estado miembro adoptar medidas contra un PSSI establecido en otro Estado miembro, cuya actividad se dirige principalmente o en su totalidad hacia el territorio del primero, siempre que «[…] dicho establecimiento se haya realizado con la intención de evadir la legislación que se hubiera aplicado al prestador de servicios en caso de que se hubiera establecido en el territorio del primer Estado miembro» –considerando 57 DCE–.

En segundo lugar –artículo 3.4.b) DCE–, con carácter previo a la adopción de estas medidas y sin perjuicio de los procesos judiciales que puedan interponerse (incluidas las actuaciones preliminares y los actos realizados en el marco de una investigación criminal), el Estado miembro habrá de pedir a su homónimo que tome las medidas necesarias para el cese de los perjuicios ocasionados o que pueda llegar a ocasionar; no siendo adoptadas o resultando estas insuficientes, deberá, como paso subsiguiente, notificar a la Comisión y al Estado miembro infractor su intención de llevarlas a cabo en nombre propio. No obstante, cuestiones de urgencia podrán habilitar al Estado miembro actuante para obviar el procedimiento

[766] Se trataba de salvaguardar, en aquel momento, la aplicación de otras Directivas comunitarias sobre protección de los consumidores, como la DADLRAEMPE (DOCE L 250, de 19 de septiembre de 1984, p. 17); la DSGP (DOCE L 228, de 11 de agosto de 1992, p. 24); la DADLRAEMCC (DOCE L 101, de 1 de abril de 1998, p. 17); la DCACCC, o la DPCCD.

[767] Como establece el considerando 10 DCE, de conformidad con el principio de proporcionalidad, «[…] las medidas previstas en la presente Directiva se limitan al mínimo necesario para conseguir el objetivo del correcto funcionamiento del mercado interior».

previsto en el párrafo anterior. En cualquier caso, las medidas que se adopten habrán de notificarse a la Comisión y al Estado miembro infractor a la mayor brevedad posible, exponiendo las razones que, a juicio de aquel, motivaban dicha celeridad (artículo 3.5 DCE).

Por lo demás, concluye el precepto tercero, corresponderá a la Comisión verificar la compatibilidad de las medidas notificadas por el Estado miembro afectado con el Derecho comunitario, también en el más breve plazo posible. Caso de alcanzar una conclusión en sentido negativo, la Comisión deberá solicitar a dicho Estado miembro que se abstenga de tomar ninguna de las medidas propuestas (supuesto del artículo 3.4 DCE) o que ponga fin lo antes posible a las ya adoptadas (supuesto del artículo 3.5 DCE).

Partiendo, como anticipábamos, de la norma comunitaria precitada, el artículo 8.1.1º LSSICE dispone que, en el caso de que un determinado SSI atente o pueda atentar contra los principios que a continuación se enumeran, los órganos competentes[768] para su protección, en ejercicio de las funciones que tengan legalmente atribuidas, podrán adoptar las medidas que sean necesarias para que, bien se interrumpa su prestación, bien se retiren los datos que los vulneran; estos principios son[769]: a) la salvaguarda del orden público, la investigación

[768] Definido en el apartado j) del anexo LSSICE (la DCE no contiene definición alguna al respecto, tampoco la LMCE), tendrá la consideración de *órgano competente* «[…] todo órgano jurisdiccional o administrativo, ya sea de la Administración General del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas». Como aclara PEGUERA POCH, M., *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010, pp. 332 y 333, esta alusión a los órganos competentes no se limita a los órganos judiciales, sino que incluye también a los órganos de naturaleza administrativa que tengan legalmente atribuida la protección de dichos principios; ello, añade, no debe interpretarse como una atribución por la LSSICE a las autoridades administrativas de una competencia general para velar por la licitud de los SSI, sino que se limita a establecer que aquellos órganos que ya tengan previamente encomendada la protección administrativa de los mismos puedan adoptar las medidas previstas que resulten necesarias, encaminadas, como decimos, a interrumpir la prestación del servicio o a retirar los datos que vulneran tales principios. En la misma línea, señala el artículo 35.1.2º LSSICE, «[…] las referencias a los órganos competentes contenidas en los artículos 8, 10, 11, 15, 16, 17 y 38 se entenderán hechas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia».

[769] Como podremos observar a continuación, si comparamos este apartado primero del artículo 8 LSSICE con su homónimo 3.4 DCE, vemos que se han añadido dos importantes previsiones no contempladas a nivel comunitario: se trata de la inclusión del principio de no discriminación por motivos de opinión, discapacidad o

penal, la seguridad jurídica y la defensa nacional; b) la protección de la salud pública o de las personas físicas o jurídicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores; c) el respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social; d) la protección de la juventud y de la infancia, y e) la salvaguarda de los derechos de propiedad intelectual[770]. En la adopción y cumplimiento de estas medidas se respetarán, en todo caso, las garantías, normas y procedimientos contemplados en el ordenamiento jurídico para proteger, cuando pudieran resultar afectados, los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión o a la libertad de información; asimismo, en aquellos casos en que la CE y las leyes que regulen los respectivos derechos y libertades así lo prevean de manera excluyente, tan sólo la autoridad judicial competente, «[…] en tanto garante del derecho a la libertad de expresión, del derecho de producción y creación literaria, artística, científica y técnica, la libertad de cátedra y el derecho de información» podrá adoptar estas medidas de restricción (artículo 8.1.2º y 3º LSSICE)[771].

La LSSICE prevé también una importante atribución, centrada en la posibilidad con que cuentan estos órganos competentes para, con el fin de identificar al responsable del SSI que está realizando la conducta presuntamente vulneradora y que este pueda comparecer en el

cualquier otra circunstancia personal o social –apartado c)– y la salvaguarda de los derechos de propiedad intelectual –apartado e)–.

[770] En torno a la cuestión de la salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los PSSI (incluidos los PSSIi), *vid.* CARBAJO CASCÓN, F., «Aspectos sustantivos del procedimiento administrativo para la salvaguarda de derechos de propiedad intelectual en Internet», cit., pp. 7 y ss.

[771] Podemos ver en la previsión del artículo 8.1.3º LSSICE una preocupación del legislador por dejar claro que esta posibilidad de imponer restricciones a la prestación de SSI no podrá ir en detrimento del ejercicio de los derechos y libertades enunciados, que no son otros que los reconocidos y protegidos en el artículo 20.1 CE. En todo caso, no podemos obviar que el ámbito que ha de quedar reservado a las autoridades judiciales y, en consecuencia, el correlativo campo de actuación de los órganos administrativos, no resulta fácil de delimitar en la práctica, habida cuenta de la íntima conexión con la libertad de expresión e información que, en muchos casos, presentarán los SSI, en particular los prestados a través de páginas web.

procedimiento, requerir a los PSSI (en nuestro caso, PSSIic) la cesión de los datos que permitan tal identificación. Este requerimiento exigirá de una previa autorización judicial, de conformidad con lo dispuesto en el artículo 122 bis.1 LJCA[772] (artículo 8.2 LSSICE).

Ahora bien, dispone el artículo 8.3 LSSICE, para la adopción de restricciones a la prestación de SSI provenientes de PSSI (PSSIisc) establecidos en un Estado miembro de la UE o del EEE distinto a España, deberá seguirse el procedimiento de cooperación intracomunitario que se describe en el artículo 8.4 LSSICE, sin perjuicio de cuanto pueda disponerse en la legislación procesal y de cooperación judicial. De acuerdo con dicho procedimiento, y en términos similares a como hiciera el antes descrito artículo 3.4 DCE, el órgano competente deberá requerir al Estado miembro en que esté establecido el PSSI afectado para que adopte las medidas oportunas; caso de que estas medidas no sean adoptadas o, siéndolo, devengan insuficientes, dicho órgano competente notificará, con carácter previo, las medidas que tiene intención de adoptar, notificación que habrá de hacerse a la Comisión Europea (o, en su caso, al Comité Mixto del EEE) y al Estado miembro de que se trate –artículo 8.4.a) LSSICE–; ahora bien, en casos de urgencia, el órgano competente podrá adoptar las medidas de restricción que estime convenientes sin necesidad de notificarlo, debiendo hacerlo posteriormente (a la mayor brevedad y, en cualquier caso, en el plazo máximo de quince días desde su adopción), tanto al Estado miembro de que se trate como a la Comisión Europea (o, en su caso, al Comité Mixto del EEE), haciendo constar las causas que motivaron dicha urgencia –artículo 8.4.b) LSSICE–. Los requerimientos y notificaciones aludidos «[…] se realizarán siempre a través del órgano de la Administración General del Estado competente para la comunicación y transmisión de información a las Comunidades Europeas» (artículo 8.4, *in fine*, LSSICE)[773]. Del lado inverso, los órganos competentes de otros Estados miembros de la UE o del EEE podrán requerir también la colaboración de PSSIi establecidos en España,

[772] BOE núm. 167, de 14 de julio de 1998. De acuerdo con este precepto, añadido en virtud de la D. F. 43.7 LES, «[e]l procedimiento para obtener la autorización judicial a que se refiere el artículo 8.2 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico, se iniciará con la solicitud de los órganos competentes en la que se expondrán las razones que justifican la petición acompañada de los documentos que sean procedentes a estos efectos. El Juzgado, en el plazo de 24 horas siguientes a la petición y, previa audiencia del Ministerio Fiscal, dictará resolución autorizando la solicitud efectuada siempre que no resulte afectado el artículo 18 apartados 1 y 3 de la Constitución».

[773] Nada se dice en la LSSICE de la previsión que, en cambio, sí recoge el artículo 3.6 DCE, plenamente aplicable, en cualquier caso.

en términos similares a los previstos en el artículo 11.2 LSSICE, si así lo consideran necesario para garantizar la eficacia de las medidas de restricción que adopten al amparo del artículo 8.4 LSSICE (artículo 8.5 LSSICE).

Asimismo, las medidas de restricción que, en su caso, se adopten al amparo de este artículo deberán cumplir siempre las garantías y los requisitos previstos en el artículo 11.3 y 4 LSSICE (artículo 8.6 LSSICE).

Por último, el artículo 5 LFE, aún en vigor tras la promulgación del RIE-SCTE (cuyo artículo 4 regula en la actualidad este principio a nivel de la UE[774]), subraya este principio al establecer que la prestación de SSIic «[…] se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo».

Como reglas comunes a los principios de aplicación de la ley del país de origen y de reconocimiento mutuo o de libre prestación de SSI, la DCE prevé una serie de ámbitos a los que no se aplicarán los principios contemplados en el artículo 3, apartados 1 y 2, DCE; estos ámbitos son (artículo 3.3 DCE, que se remite, a su vez, al anexo de la Directiva): a) derechos de autor, derechos afines y derechos mencionados en la DPJTPS[775] y en la DPJBD[776], así como a los derechos de propiedad industrial –esta letra se corresponde, en parte, con la letra a) del artículo 3.1 LSSICE–; b) emisión de moneda electrónica por parte de instituciones a las que los Estados miembros hayan aplicado una de las excepciones previstas en el artículo 8.1 DAAEDESCE[777] –esta letra no encuentra su correlativa plasmación en el artículo 3.1 LSSICE–; c) apartado 2 del artículo 44 DCDLRADOICVM[778] –esta letra se corresponde

[774] De acuerdo con este precepto, «[n]o se impondrá restricción alguna a la prestación de servicios de confianza en el territorio de un Estado miembro por un prestador de servicios de confianza establecido en otro Estado miembro por razones que entren en los ámbitos cubiertos por el presente Reglamento. Se permitirá la libre circulación en el mercado interior de los productos y servicios de confianza que se ajusten al presente Reglamento».

[775] DOCE L 24, de 27 de enero de 1987, p. 36.

[776] DOCE L 77, de 27 de marzo de 1996, p. 20.

[777] DOCE L 275, de 27 de octubre de 2000, p. 39.

[778] DOCE L 375, de 31 de diciembre de 1985, p. 3.

con la letra b) del artículo 3.1 LSSICE–; d) artículo 30 y Título DCDLRASDDSV(II)[779], Título IV DCDLRASDV(II)[780], artículos 7 y 8 DCDLRASDDSV(I)[781] y artículo 4 DCDLRASDV(I)[782] –esta letra se corresponde con la letra c) del artículo 3.1 LSSICE–; e) libertad de las partes de elegir la legislación aplicable a su contrato –esta letra se corresponde con la letra e) del artículo 3.1 LSSICE–[783]; f) obligaciones contractuales relativas a contratos celebrados por los consumidores[784] –esta letra se corresponde la letra d) del artículo 3.1 LSSICE–; g) validez formal de los contratos por los que se crean o transfieren derechos en materia de propiedad inmobiliaria, en caso de que dichos contratos estén sujetos a requisitos formales obligatorios en virtud de la legislación del Estado miembro en el que esté situada la propiedad inmobiliaria[785] –esta letra no encuentra su correlativa plasmación en el artículo 3.1 LSSICE–, y h) licitud de las comunicaciones comerciales no solicitadas por correo electrónico[786] –esta letra se corresponde la letra f) del artículo 3.1 LSSICE–.

En todas estas materias, los PSSI (PSSIisc) establecidos en otros países de la UE o del EEE quedarán sujetos a la normativa española; no obstante, como dijimos, se exceptúan

[779] DOCE L 228, de 11 de agosto de 1992, p. 1.

[780] DOCE L 360, de 9 de diciembre de 1992, p. 1.

[781] DOCE L 172, de 4 de julio de 1988, p.1.

[782] DOCE L 330, de 29 de noviembre de 1990, p. 50.

[783] Como hace constar GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, cit., p. 235, esta cuestión se venía regulando por el CLAOC (DOCE L 266, de 9 de octubre de 1980, p. 1) que, para los contratos celebrados con posterioridad al 17 de diciembre de 2009, se regirá por el RRI, que, tal y como dispone en sus artículos 24 y 28, sustituye a dicho Convenio.

[784] En lo esencial, regidas por la DCDSFDC y por la DDC.

[785] Excepción lógica, en palabras de *Ibid.*, p. 236, por razones de seguridad jurídica, dada la naturaleza singular de dichos bienes.

[786] El objetivo era abrir la posibilidad de establecer limitaciones respecto de comunicaciones comerciales no solicitadas y llevadas a cabo por medios distintos de los electrónicos; sin embargo, la regulación posterior, contenida en el artículo 13 DPCE, que equipara en sus efectos las comunicaciones comerciales no solicitadas practicadas por vía telefónica o por fax a las electrónicas, ha dejado sin virtualidad esta excepción (*Ibid.*, p. 236).

aquellos casos en que, de conformidad con las propias normas reguladoras de dichas materias, la ley del país de residencia (o, lo que es lo mismo, del establecimiento del DSSI) no resulta aplicable (artículo 3.4 LSSICE).

### 3.1.3. Principio de no sujeción a autorización previa

Para concluir, el artículo 4 DCE disecciona otro principio esencial en el desarrollo de la actividad de los PSSI. Se trata del principio de no sujeción a autorización previa, en virtud del cual se establece la obligación por los Estados miembros de evitar que el acceso a esta profesión tenga que someterse a ningún tipo de aprobación anterior al inicio de la actividad u otro requisito equivalente; ello, empero, no irá en perjuicio de los regímenes de autorización que no tengan como objeto específico y exclusivo los SSI, ni de los regímenes cubiertos por la DMCAGLIST[787].

Este principio, ratificado específicamente para los PSSIic por el artículo 3.1 DFE[788], experimenta una notable transformación con el RIE-SCTE, cuyo precepto 21 –también el artículo 17.3.a)–, que, contraviniendo ambas Directivas comunitarias precedentes, exige, como vimos, que aquellos PSSIisc sin cualificación que tengan la intención de iniciar la prestación de SSIisc de carácter cualificado presenten al organismo de evaluación una notificación manifestando esta intención junto con un informe de evaluación de la conformidad expedido por un organismo de evaluación de la conformidad, haciéndose depender dicha prestación de la concesión de la cualificación y de la consecuente actualización de las listas de confianza

[787] DOCE L 117, de 7 de mayo de 1997, p. 15. La obligación de los Estados miembros de no someter el acceso al ejercicio de la actividad de los PSSI a autorización previa tampoco se referirá a los servicios postales recogidos en la DNCDMISPCMCS (DOCE L 15, de 21 de enero de 1998, p. 14), «[…] consistentes en el reparto físico de mensajes impresos de correo electrónico y que no afecta a los regímenes de acreditación voluntaria, en particular para los prestadores de servicios de certificación de firma electrónica» –considerando 28 DCE–.

[788] Así lo anuncia el considerando 10 DFE: «[…] El mercado interior permite a los proveedores de servicios de certificación llevar a cabo sus actividades transfronterizas para acrecentar su competitividad y, de ese modo, ofrecer a los consumidores y a las empresas nuevas posibilidades de intercambiar información y comerciar electrónicamente de una forma segura, con independencia de las fronteras. Con objeto de estimular la prestación de servicios de certificación en toda la Comunidad a través de redes abiertas, los proveedores de servicios de certificación deben tener libertad para prestar sus servicios sin autorización previa. *La autorización previa implica no sólo el permiso que ha de obtener el proveedor de servicios de certificación interesado en virtud de una decisión de las autoridades nacionales antes de que se le permita prestar sus servicios de certificación, sino también cualesquiera otras medidas que tengan ese mismo efecto*» (la cursiva es propia).

a que se refiere el artículo 22 Reglamento eIDAS. Así las cosas, contradiciendo lo dispuesto por el principio de no sujeción a autorización previa de forma general para todos los PSSI por la DCE[789] y derogando cuanto, en la misma línea, establecía de forma específica la DFE para los PSSIic, el RIE-SCTE introduce dicha autorización para los PSSIisc, pero no para todos, sino tan sólo para aquellos que pretendan prestar SSIic cualificados, manteniéndose inalterable la precitada previsión para los PSSIisc no cualificados, que no requerirán de tal autorización para el ejercicio de su actividad[790].

Pese a la lógica que encuentra esta nueva previsión, comprensible en aras de otorgar una mayor seguridad jurídica (probablemente también técnica) a los DSSIisc que contraten con el PSSIisc aquellos SSIic cualificados, encuentro inadecuado el modo en que se ve articulada,

[789] Así lo reitera el párrafo tercero del apartado II de la Exposición de Motivos del ALSEC, que pone de manifiesto «[…] la introducción por el Reglamento (UE) 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, de un régimen de autorización previa para la prestación de estos servicios», refiriéndose a los SSIisc cualificados. También, más explícitamente, el párrafo primero del apartado IV de dicha Exposición de Motivos, que añade que «[e]l Reglamento (UE) nº 910/2014 del Parlamento europeo y del Consejo, de 23 de julio de 2014, prevé, para los servicios cualificados, un sistema de autorización previa en sustitución de la comunicación instaurada en la Directiva 1999/93/CE del Parlamento europeo y del Consejo, de 13 de diciembre de 1999. Así, se establece un sistema mixto de colaboración público-privada en la supervisión de los prestadores cualificados, pues su inclusión en la lista de confianza de prestadores cualificados de servicios electrónicos establecidos en España, que permite iniciar esa actividad, debe basarse en un informe de evaluación de la conformidad emitido por un organismo de evaluación de la conformidad acreditado por un organismo nacional de acreditación establecido en alguno de los Estados Miembros de la Unión Europea. A partir de entonces, deberán remitir el citado informe al menos cada 24 meses».

[790] De nuevo, la Exposición de Motivos del ALSEC, esta vez en el párrafo segundo del apartado IV, corrobora abiertamente esta afirmación al establecer que «[…] los prestadores de servicios no cualificados pueden prestar servicios sin autorización previa, sin perjuicio de su sujeción a las potestades de monitorización y control posterior de la Administración. No obstante, deberán comunicar al órgano supervisor la prestación del servicio en el plazo de tres meses desde que inicien su actividad, a los meros efectos de conocer su existencia y posibilitar su supervisión. Por ello, la citada comunicación no equivale a la comunicación prevista en el artículo 69.2 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que sí tiene efectos autorizatorios». A raíz de esta previsión, surge el artículo 15 ALSEC, que, con base en el artículo 17.3.b) RIE-SCTE, reitera lo anterior, al disponer que los PSSIisc no cualificados no necesitarán de autorización administrativa para iniciar su actividad, pero deberán comunicar su actividad al Ministerio de Energía, Turismo y Agenda Digital (organismo de supervisión del Estado español según el Anteproyecto) en el plazo de tres meses desde que la inicien. En el mismo plazo deberán comunicar la modificación de los datos inicialmente transmitidos y el cese de su actividad».

ya que, en mi opinión, debería haber ido precedida de una previa adaptación de la normativa comunitaria de referencia, personificada en la DCE. En efecto, si lo que se pretende es alterar el principio, tradicional en el ámbito de la sociedad de la información, de no sujeción a autorización previa, únicamente para aquellos PSSI que ejerzan funciones de naturaleza intermediadora consistente en la prestación de SSIisc, hubiera sido aconsejable, para una mayor certeza y seguridad en el jurista y en todo aquel que se vea afectado por la nueva regulación, dotar de una mayor coherencia la relación entre ambas normas, bien estableciendo en la general la excepción referida, bien haciéndola constar en la específica; de lo contrario, la seguridad jurídica perseguida con la alteración del mencionado principio puede verse anulada con la inseguridad jurídica propiciada por esta incongruencia o incompatibilidad. De optar por la primera de las opciones (probablemente la más acertada), la fórmula legal empleada para solventar esta cuestión podría haber quedado redactada en los siguientes términos: *los Estados miembros dispondrán que el acceso a la actividad de prestador de servicios de la sociedad de la información no pueda someterse a autorización previa ni a ningún otro requisito con efectos equivalentes, salvo para el caso de aquellos prestadores de servicios de la sociedad de la información que ejerzan funciones de intermediación consistentes en prestar servicios electrónicos de confianza cualificados, en cuyo caso el inicio de su actividad estará condicionado a cuanto disponen los artículos 17.3.a) y 21 del Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo de 23 de junio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE*. En cualquier caso, dadas las circunstancias y en tanto no se lleve a cabo la modificación apuntada, habremos de acudir de nuevo al principio general del Derecho de especialidad normativa (*lex specialis derogat legi generali*) y al principio de temporalidad o cronología (*lex posterior derogat legi priori*) para concluir que, si bien la regla general para todos los PSSI es la no exigencia de autorización previa, sí que será necesaria la misma para aquellos PSSIisc que pretendan comenzar a prestar SSIisc cualificados.

Inevitablemente, la situación descrita tiene su propio impacto en España, donde, hasta el momento, el artículo 6 LSSICE, partiendo del originario artículo 4.1 RDLFE, se limita a afirmar que la prestación de SSI no estará sujeta a autorización previa alguna; a ello añade, como ya hiciera la DCE, la advertencia de que ello no afectará a los regímenes de autorización que estén previstos en el ordenamiento jurídico y que no tengan por objeto específico y

exclusivo la prestación por vía electrónica de SSI[791]. En la misma línea se sitúa el artículo 5.1, *ab initio*, LFE.

Sin embargo, como consecuencia de la entrada en vigor del RIE-SCTE y hasta tanto no tenga lugar la derogación definitiva de la LFE y la presumible incorporación del actual Anteproyecto, hemos de entender derogada la previsión específica contenida en el artículo 5 LFE e interpretar conjuntamente el Reglamento eIDAS junto con la DCE y la LSSICE. De este modo, alcanzamos la conclusión, antes apuntada, de considerar vigente el principio de no sujeción a autorización previa con carácter general salvo para el supuesto de PSSIisc cualificados.

### 3.2. Obligaciones

El mundo virtual, para poder llegar a convertirse en cauce elemental por el que vehicular relaciones de naturaleza plural, también necesita de la articulación de mecanismos que permitan inferir la confianza necesaria en el nuevo escenario por medio de la imposición de obligaciones y la atribución de responsabilidades a los encargados de articular su funcionamiento práctico. A su vez, y en lo que aquí interesa, para fortalecer la eficacia específica de los instrumentos de firma electrónica, debemos generar certeza en las partes implicadas delimitando el concreto campo del deber, general y específico, de los PSSIisc cualificados y no cualificados que, en esta tarea de intermediación, ayudan a la satisfacción de importantes necesidades derivadas del desarrollo de actividades de contratación (en el **anexo XXVIII** aparece la clasificación, ordenada según un criterio creciente de especificidad, de obligaciones actuales a cumplir por los PSSIisc).

#### 3.2.1. Generales o comunes a todos los prestadores de servicios de la sociedad de la información

En primer lugar, sobre todos los PSSI (cualificados y no cualificados, principales e intermediarios) pesa una *obligación de información general* que se encuentra recogida en los artículos 5

[791] Sobre esta cuestión, *vid.* CACHAFEIRO GARCÍA, F./GARCÍA PÉREZ, R., «No sujeción a autorización previa de la prestación de servicios de la sociedad de la información (comentario al art. 6 de la LSSICE)», *Revista de la contratación electrónica*, vol. 45, 2004, pp. 39 a 56.

DCE y 10 LSSICE[792]. Es esta una obligación que, reiterando los códigos de conducta elaborados en materia de comercio electrónico[793], encuentra su fundamento último en la necesidad de informar al DSSI sobre elementos de esencial importancia para la identificación[794] y localización del PSSI, ya que la apariencia generada por los nombres de dominio (primera información a la que acceden DSSI y autoridades competentes) no es del todo suficiente para suscitar la certidumbre requerida en estos casos[795]. Y es que, como de manera clara expone GERBOLÉS RODRÍGUEZ[796], «[…] cuando nos movemos en el mundo físico, vemos una tienda con su nombre comercial, su ubicación física, entramos en ella, nos atiende una persona física, nos resuelve las cuestiones que se nos puedan plantear respecto de los productos o servicios que nos ofrecen y sobre los que nosotros podemos estar interesados y nos marchamos seguros y confiados de lo que hemos visto y escuchado, en su caso. La obligación

[792] En virtud del artículo 4.3 LMISI se suprime la obligación establecida en el artículo 9 LSSICE, sobre constancia registral del nombre de dominio, «[…] dado que se ha revelado como poco operativa desde un punto de vista práctico» (párrafo noveno del apartado III de la Exposición de Motivos de la LMISI). En coherencia con esta supresión, se elimina también la originaria letra a) del apartado 4 del artículo 38 LSSICE, en la que se tipificaba como infracción administrativa leve «[l]a falta de comunicación al registro público en que estén inscritos, de acuerdo con lo establecido en el artículo 9, del nombre o nombres de dominio o direcciones de Internet que empleen para la prestación de servicios de la sociedad de la información». No consta, pero también quedaría sin efecto lo dispuesto al respecto en el párrafo primero del apartado III de la Exposición de Motivos de la LSSICE. Por último, se plantea la duda de si seguiría en vigor la D. A. 6ª LSSICE, que regula el sistema de asignación de nombres de dominio bajo el «.es».

[793] LÓPEZ JIMÉNEZ, D./MARTÍNEZ LÓPEZ, F. J., «La formación del contrato electrónico», *Revista de la contratación electrónica*, vol. 105, 2009, p. 27.

[794] Como acertadamente apunta PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, cit., p. 69, la información que se exige a los PSSI contrasta con la nula regulación respecto a la identificación de los particulares que colocan contenidos en la Red; en este sentido, afirma, «[…] debería de exigirse que cualquier página web de contenido no comercial permitiese la rápida identificación de su titular responsable con el fin de poderle dirigir las reclamaciones y sugerencias por parte del resto de usuarios que se pudieran ver directa o indirectamente perjudicados o afectados por el contenido. Sin embargo, lo bien cierto es que a fecha de hoy no existe ninguna normativa que exija la identificación de un titular de una página cuando este no es un PSSI y en muchos pleitos que se dirigen contra los PSSIi se hace así por la dificultad de identificar al titular responsable».

[795] MÁRQUEZ LOBILLO, P., *Empresarios y profesionales en la sociedad de la información*, cit., p. 193.

[796] GERBOLÉS RODRÍGUEZ, S., «Comentario a los artículos 27, 28 y 29», en CREMADES GARCÍA, J./GONZÁLEZ MONTES, J. L. (coords.) *La nueva ley de Internet: comentarios a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, Las Rozas, La Ley, 2003,, p. 432.

que vamos a analizar en este apartado persigue aportar un poco de esa confianza que, a veces, como usuarios de la Red, nos falta»; se trata, en definitiva, de intentar salvar la distancia que el desarrollo de estos SSI produce al tener lugar con ausencia física simultánea de las partes. Desde la perspectiva del consumidor, la importancia de esta obligación como instrumento de protección ha sido destacada por el Tribunal de Justicia, que, en su sentencia de 16 de octubre de 2008[797], subrayó que el suministro de esta información básica permite al DSSI apreciar el alcance de sus futuras obligaciones, reduciéndose el riesgo de celebración de contratos para ellos perjudiciales.

Así las cosas, dispone el apartado primero del artículo 5 DCE que, amén de otros requisitos en materia de información contenidos en el Derecho comunitario, los Estados miembros habrán de garantizar que el PSSI permita a los DSSI y a las autoridades competentes acceder de manera fácil, directa y permanente, como mínimo, a los datos que aparecen a continuación: a) nombre del PSSI; b) dirección geográfica en que está establecido; c) señas que permitan ponerse en contacto rápidamente con él y establecer una comunicación directa y efectiva, incluyendo su dirección de correo electrónico; d) si el PSSI está inscrito en un registro mercantil u otro registro público similar, nombre de dicho registro y número de inscripción asignado en él al PSSI u otros medios equivalentes de identificación en el registro; e) si una determinada actividad está sujeta a un régimen de autorización (al amparo del artículo 4.2 DCE), los datos de la autoridad de supervisión correspondiente; f) en lo que se refiere a las profesiones reguladas[798], si el PSSI pertenece a un colegio profesional o institución similar, datos de dicho colegio o institución, y, para todos los casos, título profesional

[797] STJUE C-298/07, de 16 de octubre de 2008, *Bundesverband der Verbraucherzentralen y Verbraucherverbände*, F. J. 22º.

[798] Para la conceptualización del término *profesión regulada*, el artículo 2.g), DCE se remite, a su vez, a dos Directivas comunitarias anteriores, cada una de las cuales contiene una definición del término igualmente válida a los efectos que aquí interesan: estamos hablando de la DSGRTES (DOCE L 19, de 24 de enero de 1989, p. 16) y de la DSSGRFP (DOCE L 209, de 24 de julio de 1992, p. 25). Por lo que respecta a la primera de ellas, afirma su artículo 1.d) que será una *actividad profesional regulada* aquella «[…] actividad profesional cuyo acceso, ejercicio o alguna de sus modalidades de ejercicio en un Estado miembro estén sometidas directa o indirectamente, en virtud de disposiciones legales, reglamentarias o administrativas, a la posesión de un título. Constituye, en especial, una modalidad de ejercicio de una actividad profesional regulada: el ejercicio de una actividad al amparo de un título profesional, en la medida en que sólo se autorice a ostentar dicho título a quienes se encuentren en posesión de un título determinado por las disposiciones legales, reglamentarias o administrativas; el ejercicio de una actividad profesional en el ámbito de la sanidad en la medida en que el régimen nacional de Seguridad Social

expedido y el Estado miembro en el que se expidió y referencia a las normas profesionales aplicables en el Estado miembro de establecimiento y los medios de acceder a las mismas; g) por último, si el PSSI ejerce una actividad gravada con el IVA, el número de identificación a que hace referencia el apartado 1 del artículo 22 DALEMIVN[799]. Asimismo, cuando el SSI de que se trate haga referencia a precios, estos deberán indicarse claramente y sin ambigüedades, haciéndose constar, en todo caso, si en él están incluidos los impuestos y los gastos de envío (artículo 5.2 DCE)[800].

Por su parte, en España, el artículo 10.1 LSSICE efectúa una enumeración tanto más exhaustiva de los requisitos informativos que han de cumplir obligatoriamente los PSSI que se vean sujetos al ámbito de aplicación de la norma; en concreto, además del carácter gratuito

supedite la remuneración y/o el reembolso de dicha actividad a la posesión de un título». Cuando ello no resulte de aplicación, prosigue el precepto, «[…] se equiparará a una actividad profesional regulada, una actividad profesional ejercida por los miembros de una asociación u organización cuyo objetivo sea promover y mantener un nivel elevado en el ámbito profesional de que se trate y que, para alcanzar dicho objetivo, goce de un reconocimiento bajo una forma específica otorgada por un Estado miembro y que expida un título a sus miembros, dicte normas profesionales a las que habrán de atenerse sus miembros, y confiera a éstos el derecho de ostentar un título, abreviatura o condición que correspondan a tal título». La segunda de las Directivas, por su parte, contiene en su artículo 1.f) una definición prácticamente idéntica, si bien sustituyendo el término *título* por los de *titulación de formación o certificado de competencia*. Ambas Directivas han sido posteriormente derogadas y reemplazadas por la DRCP (DOUE L 255, de 30 de septiembre de 2005, p. 22), que entiende por *profesión regulada* –artículo 3.1.a)– «[…] la actividad o conjunto de actividades profesionales cuyo acceso, ejercicio o una de las modalidades de ejercicio están subordinados de manera directa o indirecta, en virtud de disposiciones legales, reglamentarias o administrativas, a la posesión de determinadas cualificaciones profesionales; en particular, se considerará modalidad de ejercicio el empleo de un título profesional limitado por disposiciones legales, reglamentarias o administrativas a quien posea una determinada cualificación profesional. Cuando la primera frase de la presente definición no sea de aplicación, las profesiones a que se hace referencia en el apartado 2 quedarán equiparadas a una profesión regulada» (este apartado segundo hace referencia –artículo 21.1 DRCP– a las actividades profesionales de médico con formación básica y médico especialista, de enfermero responsable de cuidados generales, de odontólogo, de odontólogo especialista, de veterinario, de farmacéutico y de arquitecto). En el ordenamiento jurídico español, todo ello tendrá su reflejo en la letra g) del anexo, que entiende por *profesión regulada* «[…] toda actividad que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias».

[799] DOCE L 145, de 13 de junio de 1977, p. 1.

[800] Sobre esta cuestión, *vid*. BESCÓS TORRES, M., «Formas contractuales en el comercio electrónico», *Información comercial española*, vol. 813, 2004, p. 182.

y de la posibilidad de acceder por medios electrónicos a la información relativa al PSSI[801] (también de forma fácil, directa y permanente), la LSSICE incorpora un último apartado –apartado g)– que obliga a informar de los códigos de conducta[802] a los que, en su caso, esté adherido el PSSI y la manera de consultarlos electrónicamente. Esta obligación también se entenderá satisfecha si el PSSI la incluye en su página o sitio de Internet, siempre y cuando lo haga atendiendo a las exigencias *supra* descritas (artículo 10.2 LSSICE); ello exige que la información sea proporcionada de forma claramente visible e identificable, de modo que no basta con incluirla en el sitio web si aparece tan escondida que un usuario común no podría encontrarla a menos que realizase un examen excesivamente complejo y exhaustivo, contrario a la finalidad de la Ley[803].

Este mismo precepto prevé un último apartado, no recogido en la Directiva comunitaria de referencia, que contempla aquellos supuestos en que se ha atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a SSI y se requiera su utilización por parte del PSSI. En estos casos, dicho empleo, así como la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el necesario consentimiento, previo, informado y expreso, del usuario. A tales efectos, el PSSI deberá comunicar, como mínimo y de manera claramente visible e identificable, la siguiente información: a) las características del servicio que se va a proporcionar; b) las funciones que efectuarán los programas informáticos que sean descargados, incluyendo el número telefónico que se marcará; c) el procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en el que dicho fin tendrá lugar, y d) el

[801] Ambas exigencias (gratuidad de la información y acceso a la misma por medios electrónicos) no se encuentran contempladas en la DCE, siendo añadidas por la LSSICE.

[802] Se hace patente el propósito perseguido por la LSSICE, plasmado en el párrafo cuarto del punto IV de su Exposición de Motivos, de promover la elaboración de códigos de conducta sobre las materias reguladas, toda vez que constituyen un instrumento de autorregulación especialmente adecuado para adaptar los diversos preceptos de la Ley a las características específicas de cada sector; al respecto, *vid.* LÓPEZ JIMÉNEZ, D./MARTÍNEZ LÓPEZ, F. J., «Los códigos de conducta como solución frente a la falta de seguridad en materia de comercio electrónico», *Revista de ciencias económicas*, vol. 1, 2010, pp. 117 a 139; LUNA HUERTAS, P./MARTÍNEZ LÓPEZ, F. J., «Sociedad de la información y el conocimiento y nuevos paradigmas del Derecho: el caso de los códigos de conducta en el comercio electrónico», *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, vol. 2, 2002, pp. 59 a 99.

[803] ARIAS POU, M., *Manual práctico de comercio electrónico*, cit., p. 100.

procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional. Todo ello se entenderá sin perjuicio de todo cuanto al respecto disponga la normativa de telecomunicaciones, especialmente en lo relativo a los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional.

En segundo lugar, nos remitimos a cuanto quedó indicado en los artículos 20 y 21 LSSICE al hablar, de una parte, de todo lo concerniente a las comunicaciones comerciales, ofertas promocionales y concursos, así como a las obligaciones que, en esta materia, recaen sobre los PSSI, y, de otra, a la prohibición de comunicaciones comerciales a través de correo electrónico o de medios de comunicación electrónica equivalentes.

En tercer lugar, y acudiendo de nuevo a cuanto se ha dicho al respecto dentro de la presente obra, la *obligación de todo PSSI de habilitar procedimientos sencillos y gratuitos para que los DSSI puedan revocar el consentimiento que hubieran prestado para la recepción de comunicaciones comerciales* (artículo 22 LSSICE).

En cuarto lugar, y finalizando con los deberes que, con carácter amplio, afectan a todo aquel que asuma tareas de PSSI, se encuentra la *obligación de colaboración general* que sobre estos recae, recogida en el ámbito del Derecho comunitario en el artículo 19.1, *in fine*, DCE y, en el Derecho español, en los artículos 8.2 (ya visto) y 36 LSSICE. Este último precepto (sobre la base del primero[804]) exige a los PSSI que faciliten al Ministerio de Ciencia y Tecnología[805] y a los demás órganos a que se refiere el artículo 35 LSSICE[806] toda la información y colaboración que resulten precisas para el ejercicio de sus funciones; además de ello, prosigue el apartado primero, dichos PSSI «[…] deberán permitir a sus agentes o al personal inspector

[804] Según el artículo 19.1 DCE, «[l]os Estados miembros dispondrán de los medios de control e investigación necesarios para aplicar de forma eficaz la presente Directiva y garantizarán que los prestadores de servicios comuniquen la información requerida».

[805] En la actualidad, como sabemos, Ministro de Energía, Turismo y Agenda Digital.

[806] Estos son el Ministerio de Industria, Energía y Turismo –en la actualidad, como sabemos, al Ministro de Energía, Turismo y Agenda Digital– (artículo 35.1.1º LSSICE); los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia (artículo 35.1.2º LSSICE); los funcionarios adscritos a todos los órganos anteriores (artículo 35.2 LSSICE), y los órganos a los que la legislación sectorial atribuya competencias de control, supervisión, inspección o tutela específica (artículo 35.3 LSSICE).

el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la actividad de control de que se trate», siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 LJCA. Si como consecuencia de esta actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes de ámbito estatal o autonómico, se deberá dar cuenta de tales hechos a los órganos u organismos competentes para su supervisión y sanción (artículo 36.2 LSSICE).

En quinto lugar, y cumulativamente a las anteriores[807], aquellos PSSI que realicen específicamente actividades de contratación electrónica estarán también sujetos a una *obligación de información previa a la realización de un pedido*, recogida de manera esencial en los artículos 10 DCE y 27 LSSICE. El objetivo que con ello se persigue es el de proporcionar al usuario un conocimiento completo del contenido del contrato y advertirle de los distintos pasos que se han de acompañar para que este pueda ser válido y eficaz.

Como decíamos, el artículo 10.1 DCE establece los aspectos que, complementarios a cuantos puedan existir en materia de información en el Derecho comunitario, han de ser comunicados al DSSI «[…] de manera clara, comprensible e inequívoca» antes de efectuar un pedido. Esta información, que no será necesaria cuando ambas partes del contrato actúen por motivos profesionales y así lo acuerden[808], estará integrada por los siguientes datos: a) los distintos pasos técnicos que han de seguirse para celebrar correctamente el contrato electrónico; b) si el PSSI va a registrar, o no, el contrato así celebrado y si este va a ser accesible; c) los medios técnicos que se van a suministrar para poder identificar y corregir los errores de introducción de datos antes de efectuar el pedido[809]; d) las posibles lenguas en que se podrá

[807] Y, como señala PEGUERA POCH, M., *Principios de Derecho de la sociedad de la información*, cit., p. 364, a cuantos requisitos que, previstos en otras normas, sean aplicables (como, entre otros, los requisitos que resulten de aplicación por razón de la modalidad contractual de que se trate, del tipo de servicio prestado o de las condiciones de las partes que intervengan).

[808] De ello se desprende que la información del artículo 10 DCE será imperativa para la contratación electrónica B2C (donde se pretende proteger a la parte débil del contrato) y dispositiva para la contratación electrónica distinta de la anterior (ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 246 y 247).

[809] Como advierte ARIAS POU, M., «El deber de información en la contratación electrónica», *La ley mercantil*, vol. 17, 2015, p. 3, la DCE (al igual que, como veremos, la LSSICE) no regula el tratamiento del error en la contratación electrónica, limitándose a imponer al PSSI la obligación de informar sobre los medios técnicos existentes para identificar y corregir errores en la introducción de datos previa a la realización del pedido. Por lo demás, será frecuente en estos casos que la aplicación informática muestre ventanas de confirmación en los diversos

celebrar el contrato, y (artículo 10.2) los códigos de conducta correspondientes a los que se acoja y la manera de consultarlos electrónicamente. Esta información no será exigible a aquellos contratos electrónicos que se hayan celebrado de manera exclusiva a través del intercambio de correo electrónico u otra comunicación individual equivalente (sí, por tanto, a cuantos se perfeccionen a través de páginas web), con independencia de la condición consumidora, o no, de quien actúe como DSSI[810]; la razón estriba en que, en estos casos, del lado del PSSI siempre existirá una persona (no un simple sistema automatizado) que suministre la información que, en su caso, se precise[811], además del hecho de que la actividad negocial no será tan compulsiva ni tan irreflexiva como en la contratación electrónica automática[812].

A las anteriores se añadirá la obligación de suministrar las CGC, no estableciéndose su carácter opcional en los supuestos de contratos electrónicos distintos de los B2C ni en aquellos casos en que este se celebre exclusivamente mediante el intercambio de correo electrónico u otra comunicación individual equivalente. En cualquier caso, encontramos aquí una nueva manifestación del principio de equivalencia funcional si entendemos, como parece que es lo correcto, que el predisponente cumple con esta puesta a disposición no sólo con su envío en papel sino también mediante su remisión en forma de mensaje de datos recuperable, almacenable y reproducible[813].

---

apartados del formulario de pedido, no permita proseguir si los datos de un apartado no se han proporcionado de manera adecuada y ofrezca los detalles de los bienes o servicios objeto del contrato electrónico para que puedan ser modificados por el cliente antes de la aceptación del mismo (DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., p. 49). Sobre esta cuestión, *vid.* Sentencia del Juzgado de 1ª Instancia nº 6 de Badalona núm. 106/2011, de 8 de junio.

[810] De este modo, tan sólo será preceptiva la transmisión de la referida información: a) cuando el DSSI tenga la condición de consumidor (B2C) o cuando, no teniéndola (B2B o B2A, entre otros), no acuerde con la contraparte (PSSI) la ausencia de su suministro, o b) cuando el contrato electrónico no se celebre exclusivamente mediante el intercambio de correo electrónico u otra comunicación individual equivalente.

[811] GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, cit., pp. 240 y 246; en la misma línea, MIRANDA SERRANO, L. M. Y OTROS, «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», cit., p. 87.

[812] GARCÍA MÁS, F. J. Y OTROS, «La contratación electrónica: modernidad y seguridad jurídica», cit., p. 126.

[813] ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 283 y 284.

En nuestro país, el artículo 27 LSSICE[814] añade, por lo pronto, cuatro precisiones significativas: a) se exige al PSSI que, en aquellos casos en que sea preceptivo el suministro de información, lo sea «[…] mediante técnicas adecuadas al medio de comunicación utilizado»; b) a las notas ya conocidas de claridad, comprensibilidad y ausencia de equivocación de la información a proporcionar, se añaden las de permanencia, facilidad y gratuidad, dirigidas igualmente a reforzar la confianza y la seguridad del DSSI en el procedimiento de contratación por vía electrónica; c) se concede al PSSI la posibilidad de dar por cumplida la referida obligación de puesta a disposición de información si la misma es incluida en la página web o sitio de Internet en las condiciones señaladas en el párrafo primero del precepto o, en aquellos otros casos en que el PSSI diseñe específicamente sus SSI de contratación electrónica para ser accedidos mediante dispositivos que cuenten con pantallas de formato reducido[815], si se facilita de manera permanente, fácil, directa y exacta la dirección de internet en que dicha información es puesta a disposición del DSSI[816], y d) se incorpora una precisión temporal importante, consistente en establecer que, sin perjuicio de lo que se pueda establecer en la legislación específica aplicable, las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente (PSSI)[817] o, en su defecto,

[814] Precedida por el párrafo tercero del punto III de la Exposición de Motivos de la LSSICE. Esta norma coexistirá con cuanto establece la normativa en materia de defensa de los consumidores para los supuestos de contratación a distancia (DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 48 a 55; PÉREZ BES, F., *El Derecho de Internet*, Barcelona, Atelier, 2016, p. 131).

[815] Las preguntas al respecto podrían ser varias: ¿qué se entiende por dispositivos que cuenten con pantallas de formato reducido?, ¿los teléfonos móviles solamente?, ¿también las tablets?, ¿qué sucede con los ordenadores portátiles de pequeñas dimensiones?

[816] Sobre esta cuestión, *vid.* STJUE C-419/12, de 5 de julio, *Content Services Ltd y Bundesarbeitskammer*.

[817] Ello, siguiendo a ILLESCAS ORTIZ, R., «Oferta, perfección y prueba del contrato electrónico», *Estudios de Derecho judicial*, vol. 50, 2004, pp. 225 y 226, ha de interpretarse en el sentido de que el PSSI por vía electrónica es libre para determinar el período de validez de su oferta; ahora bien, si no hace uso de esta facultad y, por ende, nada se dice al respecto en la página web donde se formula la oferta, se establece legalmente su validez durante todo el tiempo que permanezca en situación de accesibilidad. Por lo demás, esta vez en otra obra distinta, ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., pp. 260 y 261, concluye que este artículo 27.3 LSSICE resulta excesivo «[…] puesto que si consistió en un mensaje de datos recibido correctamente por su destinatario, el contenido de ese mensaje de datos va a resultar accesible a su destinatario por toda una eternidad si es que el mensaje de datos resulta archivado por aquél. Por tanto ha de entenderse que la regla de la vigencia de la oferta mientras que resulte accesible ha de aplicarse restrictivamente y más bien para ofertas (o invitaciones a ofertar) contenidas en sitios o páginas web. En este caso y en tanto que el titular de la página no

durante todo el tiempo que permanezcan accesibles a los DSSI. Por lo demás, el precepto mantiene, en modo casi idéntico, los distintos aspectos relacionados con el contrato que han de ser objeto de comunicación, a excepción del relativo a los códigos de conducta (artículo 10.2 LSSICE), que, pese a ello, entendemos plenamente exigible a las relaciones de esta naturaleza que se hallen sujetas al ordenamiento jurídico interno español.

En sexto lugar, los PSSI que desarrollen actividades negociales de forma telemática y que, por tanto, hayan de satisfacer al deber de información a que antes aludíamos, estarán igualmente compelidos a satisfacer una *obligación de información posterior a la celebración de un contrato por vía electrónica*, contemplada fundamentalmente en los artículos 11 DCE y 28 LSSICE. La finalidad última de esta exigencia es confirmar al usuario que la oferta y la aceptación de dicho contrato han concluido de manera satisfactoria.

El artículo 11 DCE fue el que más modificaciones sufrió durante la tramitación de la norma, tanto en la Propuesta de Directiva como en la Propuesta Modificada de Directiva, dejando finalmente de lado el problema que, durante su tramitación, trató de resolver, como es el del momento de perfección del contrato. En efecto, la Propuesta Modificada de Directiva, se disponía que «[…] el contrato quedará celebrado cuando el destinatario del servicio haya recibido por vía electrónica una notificación del prestador de servicios acusando recibo de la aceptación del destinatario del servicio»; de este modo, la DCE se pronunciaba en beneficio de un sistema de confirmación de la aceptación. Sin embargo, la redacción final del precepto, tal y como quedó fijada en la Posición Común de 28 de febrero de 2000, eludió cualquier pronunciamiento sobre el delicado tema del momento de perfección del contrato electrónico, dejando esta cuestión a la voluntad de los distintos Estados miembros[818].

Por lo que respecta propiamente a su contenido, dispone el apartado primero que, salvo en el supuesto de celebración de un contrato electrónico distinto del B2C en el que las partes

retire de ella la oferta o la invitación de que se trate podrá entenderse que sigue produciendo efectos procontractuales salvo que de su tenor literal pudiera inferirse una voluntad distinta. Ello es lo que puede acontecer cuando (como sucede en muchas ocasiones) en el texto de la oferta se indique que la misma seguirá en vigor en tanto duren las existencias».

[818] PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, cit., pp. 187, 188 y 194.

así lo acuerden[819], tras la realización de un pedido en línea por parte de un DSSI[820], habrán de aplicarse dos principios: de un lado, la obligación del PSSI de acusar recibo del pedido[821] al DSSI sin demora indebida[822] y por vía electrónica, no siendo aplicable la misma cuando el contrato electrónico (B2C o cualquier otro) se haya celebrado exclusivamente a través del intercambio de correo electrónico u otra comunicación individual equivalente[823]; de otro, la

[819] Así, por tanto, los supuestos en los que, de acordarlo las partes, no se aplicarán los principios que se contienen en el artículo 11.1 DCE a aquellos casos en los que el DSSI efectúe su pedido por vía electrónica serán los siguientes: en primer lugar, cuando el PSSI (que siempre ha de actuar en el marco de su actividad profesional de prestación de un SSI) sea una persona jurídica y el DSSI (siempre que esté actuando en el marco de su actividad profesional) sea una persona jurídica; en segundo lugar, cuando el PSSI sea una persona física y el DSSI (siempre que esté actuando en el marco de su actividad profesional) una persona jurídica o cuando el PSSI sea una persona jurídica y el DSSI (siempre que esté actuando en el marco de su actividad profesional) una persona física, y, en tercer lugar, cuando el PSSI sea una persona física y el DSSI (siempre que esté actuando en el marco de su actividad profesional) sea persona física.

[820] Por ejemplo, *cliqueando* sobre un icono para aceptar la oferta del PSSI.

[821] Como establece el considerando 34 DCE el acuse de recibo expedido por el PSSI puede consistir en suministrar en línea el SSI pagado. Y es que, como bien indica el párrafo 93 de la Guía para la incorporación al Derecho interno de la LMCE, la noción de *acuse de recibo* «[…] se emplea a menudo para abarcar toda una gama de procedimientos, que van desde el simple acuse de recibo de un mensaje no individualizado a la manifestación de acuerdo con el contenido de un mensaje de datos determinado». En cualquier caso, como ya pusieran de manifiesto ILLESCAS ORTIZ, R. Y OTROS, *Derecho mercantil internacional. El Derecho uniforme*, cit., p. 355, «[e]l acuse de recibo […] constituye una pieza básica del comercio electrónico en la medida en que contribuye de manera decisiva a la certidumbre respecto de la llegada de los mensajes de datos a sus destinatarios: el iniciador, en efecto, cuando recibe de su destinatario el acuse de recibo del mensaje de datos que le ha enviado precedentemente adquiere la certeza de que la comunicación que pretendía establecer con su contraparte ha sido lograda. En este sentido, el acuse de recibo resulta de enorme utilidad a los fines de certeza de llegada y recepción de los mensajes de datos. En cualquier caso el acuse de recibo contiene siempre una mera declaración de conocimiento (de la llegada del mensaje de datos del que se acusa recibo). No constituye nunca una declaración de voluntad. […] Se parte de la hipótesis, común en la vida del tráfico, de que el acuse de recibo es un mensaje de datos y que por tanto, el acuse de recibo posee soporte electrónico. Así suele acontecer pero no tiene que serlo forzosamente: el acuse de recibo podrá ser efectuado mediante otros soportes, papel principalmente, sin que ello le reste funcionalidad y eficacia».

[822] Concepto jurídico indeterminado.

[823] Y es que, a través de estos medios, se hace posible la previa individualización de las operaciones electrónicas de naturaleza contractual efectuadas, conociendo el DSSI toda la información, casi con toda seguridad, acerca de si la realización del pedido ha llegado hasta el PSSI, hecho que corroborará plenamente cuando reciba la

presunción de que el pedido y el acuse de recibo han sido realizados cuando las partes a quienes se dirigen pueden tener acceso a los mismos, aun cuando, *de facto*, dicho acceso no se haya producido[824]. De este modo, el acuse de recibo no se configura como un requisito necesario para la perfección del contrato electrónico, sino como una obligación del PSSI una vez perfeccionado este[825].

En España, el artículo 28.1 LSSICE concede al oferente (PSSI o DSSI), una vez perfeccionado el contrato electrónico, la posibilidad de confirmar la necesaria recepción de la aceptación realizada por el DSSI a través de dos medios posibles: un primero, consistente en «[e]l envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación», y un segundo, alternativo y no contemplado en la DCE, que permite la confirmación de la aceptación recibida por un medio equivalente al utilizado en el procedimiento de contratación, «[…] tan pronto como el aceptante haya completado dicho procedimiento, siempre que la confirmación pueda ser archivada por su destinatario»[826].

---

respuesta de este último (GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, cit., pp. 240 y 246).

[824] En consecuencia, como bien deduce ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, cit., p. 265, cualquiera que sea la norma nacional determinante del lugar de perfección del contrato electrónico mediante la aceptación de la oferta o realización del pedido, se ha de entender que dicho lugar ha de permitir la recepción y la accesibilidad por el DSSI del mensaje de datos contenedor de la oferta aceptada con posterioridad.

[825] PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, cit., pp. 187 y 188. Por tanto, recalca este autor (*Ibid.*, pp. 197 y 198), no constituye este un requisito para la validez de dicho contrato, que se produce con la simple emisión de la aceptación por el DSSI, de modo que simplemente cumple una función de garantía, ya que proporciona seguridad jurídica y certeza al proceso de contratación; de ahí que su incumplimiento pueda reforzarse por medio de la imposición de sanciones de naturaleza civil o administrativa.

[826] Este es el supuesto, por ejemplo, de las operaciones en que la aceptación se manifiesta haciendo *clic* sobre la página web en la que realizamos la compra y, acto seguido, aparece una nueva pantalla que nos indica que la aceptación ha sido recibida correctamente; ahora bien, esta manera de confirmar la aceptación tan sólo resultará suficiente si es susceptible de ser archivada por el DSSI (PEGUERA POCH, M., *Principios de Derecho de la sociedad de la información*, cit., pp. 368 y 369). En cualquier caso, ello facilita el cumplimiento de la obligación sin necesidad

Ahora bien, en aquellos casos en que la obligación de confirmación de la aceptación correspondiese al DSSI (supuestos en que el contrato electrónico viene precedido de una *invitatio ad offerendum* del PSSI), el PSSI facilitará el cumplimiento de la misma poniendo a disposición de aquel alguno de los dos medios precitados, siendo exigible la obligación tanto si la confirmación hubiera de dirigirse al propio PSSI como si debiera hacerlo a otro DSSI.

En cuanto al momento de la recepción de la aceptación y de la confirmación de la misma, este será aquel en el que las respectivas partes a quienes se dirijan puedan tener constancia de ello (artículo 28.2 LSSICE); en este último supuesto, si se opta por el primero de los medios indicados en el apartado primero (envío de acuse de recibo), se presumirá que su destinatario puede tener constancia de la recepción desde que el acuse haya sido almacenado, bien en el servidor en que esté dada de alta su cuenta de correo electrónico, bien en el dispositivo utilizado para la recepción de comunicaciones[827].

Por último, y al igual que hiciera la Directiva de referencia, se establece la posibilidad de eludir el cumplimiento de la obligación de confirmar la recepción de la aceptación de la oferta cuando ambos contratantes así lo acuerden y ninguno de ellos tenga la condición de consumidor o cuando el contrato se haya celebrado exclusivamente mediante el intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, siempre (he aquí otra novedad respecto de la DCE) que tales medios no sean empleados con el fin exclusivo (¿sí complementario?) de eludir el cumplimiento de tal obligación en fraude de ley[828].

### 3.2.2. Específicas o concretas de los prestadores de servicios de intermediación

Adentrándonos ya en las obligaciones propias y específicas de los PSSIi, podríamos comenzar, a fin de concatenarlas con las anteriores, con la *obligación de colaboración específica* que

---

de enviar mensaje de datos alguno, siendo suficiente con el hecho que la confirmación se muestre inmediatamente después de completar el proceso de contratación mediante una ventana en la pantalla cuya información pueda ser archivada por el aceptante (DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, cit., pp. 74 y 75).

[827] Esta solución, que tiene su origen en el artículo 11.1, *in fine*, DCE, se vincula con lo dispuesto en el artículo 15 LMCE (desarrollado en los párrafos 100 a 107 de la Guía para la incorporación al Derecho interno de la LMCE).

[828] Este inciso estaba también contemplado en el artículo 27.2.b) LSSICE, pero fue objeto de supresión merced al artículo 4.11 LMISI. Desconozco el motivo por el que se mantiene (en mi opinión, correctamente) en el artículo 28 de la norma y no en el artículo precedente.

recae sobre todos los PSSIi y que se encuentra recogida en los artículos 15.2 DCE[829] y 11 LSSICE. Indica la norma europea que los Estados miembros podrán establecer obligaciones tendentes a que los PSSIi comuniquen con prontitud[830] a las autoridades públicas competentes los presuntos datos ilícitos o las actividades ilícitas llevadas a cabo por sus DSSIi[831]. Sobre esta base, realiza el artículo 11 LSSICE una separación de supuestos, según el PSSI afectado por la interrupción en la prestación del SSI o por la retirada de determinados contenidos (medidas estas que, reguladas en el artículo 8 LSSICE, deberán ser siempre objetivas, proporcionadas[832] y no discriminatorias, adoptándose de forma cautelar o en ejecución de las resoluciones que se dicten, conforme a los procedimientos administrativos legalmente establecidos o a los previstos en la legislación procesal que corresponda –artículo 11.4 LSSICE–[833]) se halle establecido en España (artículo 2 LSSICE[834]) o lo esté fuera de nuestras fronteras y fuera de la UE/EEE (artículo 4 LSSICE)[835]: a) en relación con el primero de los supuestos,

[829] No se trata de imponer un deber de vigilancia general de los contenidos que se introduzcan o existan en la Red, ya que, al amparo de este precepto de la normativa comunitaria, se impide que los Estados miembros puedan imponer a los PSSIi una obligación de supervisión ni de búsqueda al respecto (MÁRQUEZ LOBILLO, P., *Empresarios y profesionales en la sociedad de la información*, cit., p. 198).

[830] De nuevo, concepto jurídico indeterminado, a especificar por la normativa nacional de desarrollo.

[831] Prosigue el precepto estableciendo la obligación, específica de aquellos PSSIi que realicen tareas de almacenamiento –no siendo aplicable, en principio, a los PSSIisc, pues no parece identificarse esta actividad con ninguna de las recogidas en el artículo 3.16)–, de comunicar a las autoridades competentes, a solicitud de estas (requisito *sine qua non*, no exigido para la obligación del artículo 15.2, *ab initio*, DCE), información que les permita identificar a sus DSSIi con los que hayan celebrado acuerdos de almacenamiento.

[832] De acuerdo con el principio de proporcionalidad, las medidas previstas se limitarán al mínimo que resulte necesario para conseguir el objetivo del correcto funcionamiento del mercado interior (considerando 10 DCE).

[833] Sobre esta cuestión, *vid. Ibid.*, p. 198.

[834] En mi opinión, hemos de optar por una interpretación extensiva del artículo 11.1 LSSICE, exigiendo la colaboración de los PSSIi también en aquellos casos en que se ordene la interrupción en la prestación de SSI o la retirada de determinados contenidos a PSSI que, residentes o domiciliados en otro Estado (sea un Estado miembro o no), ofrezcan SSI a través de un establecimiento permanente situado en España (artículo 2.2 LSSICE).

[835] Recordemos, la colaboración de los PSSIi en aquellos casos en que se ordene la interrupción en la prestación de SSI o la retirada de determinados contenidos a PSSI establecidos en otro Estado miembro de la UE/EEE distinto a España (artículo 3 LSSICE) se halla regulada en el artículo 8.5 LSSICE, no en el artículo 11 LSSICE (desconozco a qué se debe esta, *a priori*, inadecuada ubicación).

dispone el apartado primero del precepto que, cuando un órgano competente, en ejercicio de las competencias que legalmente tiene atribuidas, adopte la precitada decisión, y para ello fuera necesaria la colaboración de los PSSIi[836], dicho órgano podrá ordenar a estos últimos que suspendan el correspondiente SSIi (en nuestro caso, SSIisc) utilizado para la prestación del SSI (como pudiera ser un contrato electrónico) o de los contenidos cuya interrupción o retirada hayan sido ordenados respectivamente; b) en relación con el segundo, añade el apartado segundo que, si para garantizar la efectividad de la resolución que acuerde tal decisión, el órgano competente estimara necesario impedir el acceso desde España a tales PSSI, y para ello fuera necesaria la colaboración de los PSSIi establecidos en nuestro país, dicho órgano podrá ordenar a estos PSSIi que suspendan el correspondiente SSIi utilizado para la provisión del SSI o de los contenidos cuya interrupción o retirada han sido ordenados respectivamente[837]. En la adopción y cumplimiento de las medidas incluidas en ambos supuestos se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger, cuando pudieran resultar afectados, los derechos a la intimidad personal y familiar, a la protección de los datos personales, a la libertad de expresión[838] o a la libertad de información; asimismo, «[e]n todos los casos en que la Constitución, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales de forma excluyente para intervenir en el ejercicio de actividades o derechos, sólo la autoridad judicial competente podrá adoptar las medidas previstas en este artículo. En particular, la autorización del secuestro de páginas de Internet o de su restricción cuando ésta afecte a los derechos y libertades de expresión e información y demás amparados en los términos establecidos en el artículo

[836] A diferencia del supuesto que se describe a continuación, no se exige aquí (al menos explícitamente) que los PSSIi a los que se les impone la colaboración hayan de estar establecidos en España, aunque parece que debe ser este el sentido interpretativo que se le ha de dar a dicho apartado; en la misma línea, *vid.* PEGUERA POCH, M., *Principios de Derecho de la sociedad de la información*, cit., p. 338.

[837] De este modo, los PSSIi, aun cuando no tengan la obligación de supervisión ni de búsqueda, sí que deberán colaborar con las autoridades competentes cuando a tal fin se les requiera; así lo establece el propio Ministerio de Energía, Turismo y Agenda Digital en su página web (www.lssi.gob.es/paginas/Index.aspx).

[838] Considerando 9 DCE.

20 de la Constitución[839] solo podrá ser decidida por los órganos jurisdiccionales competentes» (artículo 11.3 LSSICE). El resumen comparativo de ámbito de aplicación, restricciones a la libre prestación de SSI y posible colaboración de PSSIi se halla recogido en el **anexo XXIX**.

### 3.2.3. Propias o singulares de los prestadores de servicios de confianza

En primer lugar, como *obligación* ya exclusiva de los PSSIisc (cualificados y no cualificados), se encuentra aquella general y *comprensiva de todo un elenco de deberes*, todos ellos recogidos en el artículo 18 LFE. Ahora bien, todos ellos vienen a exigirse tan sólo a los PSSIisc que expiden certificados electrónicos, algo que entendemos carente de toda lógica por dos motivos fundamentales: de una parte, porque del artículo 2.2 LFE se desprende la posibilidad de que los, por entonces, PSSIic pudieran prestar otros SSIic distintos de la expedición de certificados electrónicos, quedando, no entendemos bien el motivo, exentos del cumplimiento de estas obligaciones; de otra, porque, de forma específica tras la entrada en vigor del RIE-SCTE, los PSSIisc amplían el elenco de SSIisc que pueden prestar, SSIisc entre los que, al igual que sucedía con la LFE, no sólo se encuentra la expedición de certificados electrónicos relativos a tales servicios, siendo igualmente relevante para los DSSIisc de estos otros la información contenida en las letras a) a d) de dicho precepto (fuera quedarían, obviamente, las alusiones específicas a tales certificados cuando no fueran prestados).

El primero de estos deberes consiste en evitar almacenar y copiar, «[…] por sí o a través de un tercero, los datos de creación de firma de la persona a la que hayan prestado sus servicios, salvo en caso de su gestión en nombre del firmante. En este caso, se aplicarán los procedimientos y mecanismos técnicos y organizativos adecuados para garantizar que el firmante controle de modo exclusivo el uso de sus datos de creación de firma». Sólo se habilita a los PSSIisc cualificados para gestionar los datos de creación de firma electrónica en nombre del firmante, para lo cual podrán efectuar una copia de seguridad de los mismos, siempre que: a) la seguridad de los datos duplicados sea del mismo nivel que la seguridad de los datos originales, y b) que el número de datos duplicados no supere el mínimo necesario para garantizar

[839] De acuerdo con el este precepto, «[s]e reconocen y protegen los derechos: a) a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción; b) a la producción y creación literaria, artística, científica y técnica; c) a la libertad de cátedra; d) a comunicar o recibir libremente información veraz por cualquier medio de difusión». En este último supuesto, añade, la ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de dichas libertades.

la continuidad del servicio; en ningún caso podrán ser duplicados los datos de creación de firma electrónica para ninguna otra finalidad –artículo a) LFE–.

El segundo de los deberes impone proporcionar al solicitante, antes de la prestación del SSIisc[840], la siguiente información mínima, que habrá de ser gratuita, por escrito y por vía electrónica: a) las obligaciones del firmante; la forma en que han de custodiarse los datos de creación de firma electrónica; el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de tales datos, o, en su caso, de los medios que los protegen, así como información sobre los dispositivos de creación y de verificación o validación de firma electrónica que sean compatibles con los datos de firma electrónica y con el certificado electrónico que, en su caso, se expida; b) los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo; c) el método utilizado por el PSSIisc para comprobar la identidad del firmante u otros datos que figuren, en su caso, en el certificado electrónico; d) en su caso, las condiciones precisas de utilización del certificado electrónico, sus posibles límites de uso y la forma en que el PSSIisc garantiza su responsabilidad patrimonial; e) las certificaciones que, en su caso, haya obtenido el PSSIisc y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir como consecuencia del ejercicio de su actividad, y f) las demás informaciones contenidas en la declaración de prácticas de los servicios electrónicos de confianza[841]. Cualquiera de la información anterior que sea relevante para terceros afectados por los SSIisc, añade, deberá estar disponible a instancia de estos –artículo b) LFE–.

---

[840] Si bien en el precepto se dice *antes de la expedición del certificado*, tras la entrada en vigor del RIE-SCTE debemos entender sustituida esta referencia por la de *antes de la prestación del SSIisc*, expresión, esta, más acorde con la nueva regulación comunitaria.

[841] Esta declaración aparece descrita en el párrafo cuarto del punto II de la Exposición de Motivos de la norma, que establece lo siguiente: «[l]a ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos»; su regulación se encuentra recogida en el artículo 19 LFE. Sin embargo, con la entrada en vigor del Reglamento eIDAS, el término *declaración de prácticas de certificación* vendría a ser sustituido por el de *declaración de prácticas de los servicios electrónicos de confianza*; así lo anuncia, entre otros, el artículo 12 ALSEC, que regularía, de entrar en vigor, esta figura tras la nueva normativa comunitaria.

El tercero de los deberes implica la obligación de mantener un directorio actualizado de certificados electrónicos, en el que se indicarán, en su caso, aquellos certificados electrónicos expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad de dicho directorio se protegerá mediante la utilización de los mecanismos de seguridad que resulten adecuados.

El cuarto y último de estos deberes será el de garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados electrónicos que sea rápido y seguro[842].

De entrar en vigor el ALSEC, actualmente en fase de tramitación parlamentaria, incorporaría un artículo 11, cuyos apartados primero y segundo vendrían a suplir al precepto anterior, reduciendo aparentemente el número de obligaciones a satisfacer por los PSSIisc no cualificados. En efecto, dispone el artículo 11.1 del Anteproyecto que todo PSSIisc deberá publicar información veraz y acorde con la ley y con el RIE-SCTE, algo que, entendemos, se presupone y no aporta nada nuevo; sin embargo, en su apartado segundo, añade dos obligaciones fundamentales que, ahora sí, merecen una consideración algo más exhaustiva: de un lado, incurre, en mi opinión, en el mismo error de la LFE, ya que vuelve a circunscribir, sin motivo aparente alguno, el cumplimiento las obligaciones generales a satisfacer a los PSSIisc que expidan certificados electrónicos (cualificados y no cualificados); de otro, reduce estas obligaciones a dos[843], coincidentes por lo demás con las letras a) y d) del artículo 18 LFE, que, aplicadas a aquellos PSSIisc que prestan a los concretos SSIisc de firma electrónica, vendrían a ser las siguientes: a) no almacenar ni copiar, por sí o a través de un tercero, los datos de creación de firma electrónica de la persona física a la que hayan prestado sus SSIisc, salvo en el caso de su gestión en nombre del firmante; a diferencia de la LFE, no limita esta posible gestión a los PSSIisc cualificados. En cualquier caso, de realizar esta gestión, el PSSIisc deberá utilizar «[…] sistemas y productos fiables, incluidos canales de comunicación electrónica seguros, y se aplicarán procedimientos y mecanismos técnicos y organizativos adecuados, para

[842] Como también indica el precitado apartado de la Exposición de Motivos de la LFE, «[…] estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida».

[843] Bien es cierto que la segunda tan sólo afectaría a aquellos PSSIisc que expidan certificados electrónicos, no así la primera.

garantizar que el entorno sea fiable y se utilice bajo el control exclusivo del titular del certificado. Además, deberán custodiar y proteger los datos de creación de firma […] frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad»; b) disponer de un servicio de consulta sobre el estado de validez o revocación de los certificados electrónicos accesible al público. Fuera quedarían, como anticipábamos, las importantes letras b) y c) del anterior artículo 18 LFE.

En segundo lugar, sobre todos los PSSIisc recaerá la *obligación de formular una declaración de prácticas de certificación*, recogida actualmente en el artículo 19 LFE y, de forma proyectada, en el artículo 12 ALSEC. De acuerdo con la norma actual, en ella se detallarán, en el marco de la LFE y de sus disposiciones de desarrollo, «[…] las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados, las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros». La declaración de prácticas de certificación correspondiente a cada PSSIisc estará disponible al público de manera fácilmente accesible, al menos electrónicamente y de manera gratuita.

Por su parte, el artículo 12 ALSEC describe la declaración de prácticas de servicios electrónicos de confianza (nueva denominación surgida tras la promulgación del Reglamento eIDAS) como aquel documento en el que los PSSIisc «[…] describen la forma en que prestan el servicio y aseguran el cumplimiento de las obligaciones legalmente exigibles, e informan al público sobre el modo correcto de utilización de sus servicios. La declaración de prácticas estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita». Ahora bien, a diferencia de la LFE, el Anteproyecto establece una distinción (con efectos ciertamente positivos de cara a conseguir una mayor certeza jurídica) entre la obligación anterior, común a todos los PSSIisc, y la que a continuación se describe, únicamente exigible cuando el SSIisc prestado consista en la emisión de certificados electrónicos; en ella, se establece la obligación de: a) describir en la declaración las condiciones aplicables a la solicitud y expedición de un certificado, incluida la celebración de un contrato; b) detallar

los términos aplicables a la suspensión y extinción de la vigencia de los certificados electrónicos; c) informar sobre la existencia de un servicio de consulta sobre la vigencia de los certificados, y d) indicar las obligaciones del titular en el uso del certificado, la forma en que han de custodiarse los datos de creación de firma electrónica y los medios que los protegen (exigencia que, entiendo, debería haberse incluido de forma general en el apartado primero del artículo 12 ALSEC), así como cualquier recomendación útil para garantizar una buena utilización del certificado.

En tercer lugar, el *tratamiento de los datos personales* que precisen los PSSIisc (cualificados y no cualificados) para el desarrollo de su actividad (así como los órganos administrativos para el ejercicio de las funciones que les son legalmente atribuidas) *se sujetará a cuanto dispone la legislación nacional en materia de protección de datos de carácter personal y sus normas de desarrollo* (artículos 5 RIE-SCTE y 17 LFE). Esta legislación nacional se halla personificada en la actualidad en la LOPDCP, desarrollada por el RDRDLOPDCP, que encuentra su origen en la DPPFTDP, posteriormente derogada esta última por el RPPFTDP; en consecuencia, en la actualidad se encuentra en fase de tramitación el ALOPDCP, cuya D. D. Única prevé, caso de entrar en vigor, la derogación de la LOPDCP. Para la prestación de los SSIisc al público[844], los PSSIisc «[…] únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos», habiendo de ser los datos requeridos tan sólo aquellos que sean necesarios para la prestación del SSIisc, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante (artículo 17.2 LFE).

En el supuesto de que los PSSIisc consignen un seudónimo en la transacción electrónica de que se trate a solicitud del firmante, deberán constatar su verdadera identidad y conservar la documentación que la acredite; esta identidad deberá ser revelada cuando así sea solicitada por los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás

[844] Referencia que modificaría (al igual que otras tantas derivadas de esta a lo largo del precepto) la actual de la LFE de *expedición de certificados electrónicos al público*, primero porque, a tenor del artículo 2.2 de la norma, no es sólo la actividad de expedición de certificados electrónicos la que podrían realizar los anteriores PSSIic (de hecho, de acuerdo con dicha definición, podrían no realizarla y prestar, en su lugar, otros SSIic en relación con la firma electrónica), y, después, porque, tras su transformación en PSSIisc, se amplía el elenco de SSIisc que ahora pueden prestar, donde dicha expedición de certificados electrónicos sería tan sólo una de las múltiples y posibles (no necesarias) actividades a desarrollar por dichos prestadores.

supuestos previstos en el artículo 11.2 LOPDCP[845] en que así se requiera (artículo 17.3 LFE). En ningún caso, los PSSIisc incluirán en los SSIisc que presten los datos a que hace referencia el artículo 7 LOPDCP[846] (artículo 17.4 LFE).

A nivel comunitario y, como es lógico, en la misma línea indicada, se encontraba la regulación inicial contenida en el artículo 8 DFE[847], reemplazado posteriormente por el actual artículo 5 RIE-SCTE, que se limita a establecer que el tratamiento de los datos personales será conforme a lo dispuesto en la DPPFTDP, referencia que, como hemos indicado, se ha de entender sustituida por el RPPFTDP. Por lo demás, refuerza la defensa en el uso de seudónimos al establecer que, «[…] sin perjuicio de los efectos jurídicos que la legislación nacional contemple para los seudónimos, no se prohibirá su utilización en las transacciones electrónicas». Al amparo de esta previsión, surge el artículo 10 ALSEC, que, respecto del empleo de seudónimos en el uso de certificados electrónicos, reitera la necesidad de que el PSSIisc haga constar la verdadera identidad del firmante o titular del certificado[848] y conservar la

[845] En la actualidad, y tras su entrada en vigor, deberemos conjugar esta previsión con el RPPFTDP.

[846] Son los conocidos como *datos especialmente protegidos*, como los relativos a ideología, religión o creencias; sobre esta cuestión, *vid.* DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 543. En cualquier caso, como decíamos antes, será necesario compatibilizar esta previsión con las consecuencias derivadas de la entrada en vigor del RPPFTDP.

[847] Este artículo establece lo siguiente: «1. Los Estados miembros velarán por que los proveedores de servicios de certificación y los organismos nacionales competentes en materia de acreditación y supervisión cumplan los requisitos establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. 2. Los Estados miembros velarán por que los proveedores de servicios de certificación que expidan al público certificados únicamente puedan recabar datos personales directamente del titular de los datos o previo consentimiento explícito de éste, y sólo en la medida necesaria para la expedición y el mantenimiento del certificado. Los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento explícito de su titular. 3. Sin perjuicio de los efectos jurídicos concedidos a los seudónimos con arreglo al Derecho nacional, los Estados miembros no impedirán al proveedor de servicios de certificación que consigne en el certificado un seudónimo del firmante en lugar de su verdadero nombre». También, considerandos 24 y 25 DFE.

[848] Entiendo que alude a la figura del representante. No obstante, tal y como establece el artículo 6.1.b) ALSEC, el titular de un certificado de firma electrónica con atributo de representante no podrá ser identificado mediante un seudónimo, de modo que, entiendo, habría de eliminarse esta referencia y, en línea con la LFE, mantener sólo la necesidad de constatar la verdadera identidad del firmante.

documentación que la acredite, no incluyendo nada nuevo respecto del artículo 17 LFE, salvo la modificación del artículo relativo a los datos especialmente protegidos, recogidos a nivel europeo en el artículo 9 RPPFTDP bajo la denominación de *categorías especiales de datos personales*, donde se enmarcan (apartado primero) toda una suerte de datos de origen variado, como los relativos al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o concernientes a la vida sexual o las orientaciones sexuales de una persona física.

En cuarto lugar, nacida tras la promulgación del Reglamento eIDAS, está la *obligación, común a PSSIisc cualificados y no cualificados, de adoptar las medidas técnicas y organizativas adecuadas para gestionar los riesgos para la seguridad de los SSIisc prestados,* contenida en el artículo 19 RIESCTE, al que, por haber sido analizado en páginas anteriores, nos remitimos. En desarrollo de la previsión contenida en el apartado segundo de este precepto es elaborado el (en fase de tramitación) artículo 16 ALSEC, que vendría a establecería, caso de entrar finalmente en vigor, la obligación de los PSSIisc de notificar al Ministerio de Energía, Turismo y Agenda Digital las violaciones de seguridad o pérdidas de integridad que sufran, sin perjuicio de su notificación a la AEPD, si procede, o a las personas afectadas, en su caso, amén de resolver los incidentes de seguridad que les afecten; finalmente, contempla la ampliación por los PSSIisc, en un plazo máximo de 72 horas tras la resolución del incidente, la información suministrada en la notificación inicial, con arreglo a las normas de desarrollo del Reglamento eIDAS y, en su caso, las directrices y formularios que pueda establecer el *supra* citado Ministerio.

En quinto lugar, y concluyendo con las obligaciones que, específicas de los PSSIisc, afectan a todos ellos, se encuentra aquella relativa a los supuestos en que cese en su actividad. En estos casos, regulados en el artículo 21 LFE, se disponía que el PSSIisc, antes de proceder como se indica, «[…] deberá comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados. El prestador de servicios de certificación que expida

certificados electrónicos al público deberá comunicar al Ministerio de Ciencia y Tecnología, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia. Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él. Los prestadores de servicios de certificación remitirán al Ministerio de Ciencia y Tecnología con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f)[849]. Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo».

Sin embargo, amén de las críticas (poco novedosas a estas alturas) sobre la posible incompatibilidad de esta redacción con la propia de la definición de los, por entonces, denominados PSSIic (artículo 2.2 LFE), la entrada en vigor del RIE-SCTE traerá consigo, no sólo la incipiente derogación de este precepto, sino, hasta tanto ello se produzca, su adaptación a los términos de la nueva normativa comunitaria, en una redacción que podría quedar como sigue:

> *1. El prestador de servicios de confianza que vaya a cesar en su actividad deberá comunicarlo a las partes usuarias que utilicen los servicios de confianza que haya prestado. También podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de confianza que los asuma o, en caso contrario, extinguir su vigencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador de servicios de confianza al que se propone la transferencia de la gestión de los servicios de confianza.*

[849] «Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certficación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones: f) conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo».

*2. El prestador de servicios de confianza que preste tales servicios al público deberá comunicar al Ministro de Energía, Turismo y Agenda Digital, con la antelación indicada en el apartado anterior, el cese de su actividad y el destino que vaya a dar a los servicios de confianza, especificando, en su caso, si va a transferir la gestión y a quién o si se extinguirá su vigencia. Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.*

*3. Los prestadores de servicios de confianza remitirán al Ministro de Energía, Turismo y Agenda Digital, con carácter previo al cese definitivo de su actividad, la información relativa a los servicios de confianza cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f)*[850]*. Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados servicios de confianza durante un período que considere suficiente en función de las consultas efectuadas al mismo.*

Por su parte, la precitada derogación podría venir personificada por el artículo 11.3.c) ALSEC, que, en la misma línea que su predecesora, si bien circunscrita a los PSSIisc cualificados, dispone que aquellos que vayan a cesar en su actividad deberán comunicarlo a los clientes a los que presten sus SSIisc y al organismo de supervisión con una antelación mínima de dos meses al cese efectivo de la actividad. El plan de cese de tales PSSIisc cualificados podrá incluir, de nuevo, la transferencia de clientes a otro PSSIisc cualificado, «[…] una vez acreditada la ausencia de oposición de los mismos». Igualmente, comunicará al organismo de supervisión cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad; en especial, reproduce de forma prácticamente idéntica a la normativa anterior, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.

En sexto lugar, como *propias de los PSSIisc cualificados* (centradas, pues, en el sujeto) *y/o de los SSIisc cualificados que expidan* (focalizadas, en cambio, en el objeto), se encuentran *las contenidas en los artículos 24 RIE-SCTE y 20 LFE, de un lado, y en los artículos 12 y 13 LFE, de otro, respectivamente.*

[850] El artículo 20.1.f) LFE también habría de ser consecuentemente adaptado: *además de las obligaciones establecidas en este capítulo, los prestadores de servicios de confianza que presten servicios de confianza cualificados deberán cumplir las siguientes obligaciones: f) conservar registrada por cualquier medio seguro toda la información y documentación relativa a un servicio de confianza cualificado y las declaraciones de prácticas de servicios de confianza vigentes en cada momento, al menos durante 15 años contados desde el momento de su prestación.*

El artículo 24 RIE-SCTE establece una clara separación entre aquellas obligaciones a satisfacer tan sólo por los PSSIisc cualificado que presten un concreto SSIisc, como es la expedición de certificados electrónicos cualificados[851] (apartado primero), y aquellas otras, más generales, a cumplir por todo PSSIisc cualificado que preste cualquier tipo de SSIisc cualificado (apartado segundo)[852].

En el primer supuesto, el PSSIisc cualificado deberá verificar, «[…] por los medios apropiados y de acuerdo con el Derecho nacional, la identidad y, si procede, cualquier atributo específico de la persona física o jurídica a la que se expide» dicho certificado; esta verificación podrá efectuarse directamente o a través de un tercero, de conformidad con el Derecho nacional, y podrá hacerse de cualquiera de las siguientes maneras: a) en presencia de la persona física o de un representante autorizado de la persona jurídica; b) a distancia, utilizando medios de identificación electrónica para los cuales se haya garantizado la presencia de la persona física o del representante autorizado de la persona jurídica con carácter previo a la expedición del certificado electrónico cualificado, habiendo de cumplir tal medio los requisitos establecidos en el artículo 8 RIE-SCTE en relación con los niveles de seguridad *sustancial* o *alto*; c) por medio de un certificado electrónico de una firma electrónica cualificada o de un sello electrónico cualificado expedido de conformidad con las letras a) o b) anteriores, y d) utilizando otros medios de identificación electrónica reconocidos a escala nacional susceptibles de aportar una seguridad equivalente (confirmada por un organismo de evaluación de la conformidad) en términos de fiabilidad a la obtenida con la presencia física. Junto a la obligación

[851] Ya sea este de firma electrónica (supuesto en el que nos centraremos), de sello electrónico, de sello de tiempo electrónico, de servicio de entrega electrónica certificada o de autenticación de sitios web.

[852] En consecuencia, al ser la expedición de certificados electrónicos cualificados un concreto tipo de SSIisc cualificado, quien lleve a cabo tal actividad habrá de cumplir con las obligaciones contenidas tanto en el apartado primero como en el apartado segundo del artículo 24 RIE-SCTE; en cambio, el PSSIisc cualificado que lleve a cabo la realización de cualquier otro SSIisc cualificado distinto de la emisión de certificados electrónicos cualificados, sólo habrá de cumplir con las previstas en el apartado segundo. Y es esta la conclusión que, en mi opinión, cabría extraer de la interpretación de este precepto, más allá de la confusa redacción («[a]l expedir un certificado cualificado para un servicio de confianza») que lo sustenta, que parece dar a entender (de manera ciertamente contradictoria con la definición de SSIisc contenida en el artículo 3 Reglamento eIDAS), que la expedición de certificados electrónicos no constituye un SSIisc.

anterior, y con una ubicación, en mi opinión, del todo inadecuada –artículo 24.2.k) Reglamento eIDAS–, se impone al PSSIisc cualificado establecer y mantener actualizada una base de datos de certificados electrónicos cualificados.

En el segundo, el PSSIisc cualificado deberá cumplir las siguientes obligaciones: a) informar al organismo de supervisión, caso de producirse, de cualquier cambio en la prestación de SSIisc cualificados y de su intención de cesar tales actividades; b) contar con personal y, si procede, con subcontratistas, que posean los conocimientos especializados, la fiabilidad, la experiencia y las cualificaciones necesarias y que hayan recibido la formación adecuada en materia de seguridad y normas de protección de datos personales y que apliquen procedimientos administrativos y de gestión que correspondan a normas europeas o internacionales; c) con respecto al riesgo de responsabilidad por daños y perjuicios (artículo 13 RIE-SCTE), mantener recursos financieros suficientes u obtener pólizas de seguros de responsabilidad adecuadas, de conformidad con la legislación nacional; d) antes de entrar en una relación contractual (complementando, por tanto, de manera específica las obligaciones contenidas en los artículos 10 DCE y 27 LSSICE), informar a cualquier persona que desee utilizar un SSIisc cualificado de las condiciones precisas relativas a la utilización del mismo, de manera clara y comprensible, incluyendo las limitaciones a la hora de utilizarlo; e) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustenten; f) utilizar sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de tal modo que estén a disposición del público para su recuperación sólo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos, únicamente personas autorizadas puedan hacer anotaciones y modificaciones en los datos almacenados y pueda comprobarse la autenticidad de los datos; g) tomar medidas adecuadas contra la falsificación y el robo de datos; h) registrar (si se quiere, por medios electrónicos) y mantener accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del PSSIisc cualificado, toda la información pertinente referente a los datos expedidos y recibidos por dicho PSSIisc, en particular al objeto de que sirvan de prueba en procedimientos legales y para garantizar la continuidad del SSIisc cualificado[853]; i) contar con un plan de cese actualizado para garantizar la continuidad del

[853] De la letra h) del artículo 24.2 RIE-SCTE nace el, en fase de tramitación, artículo 11.3.a) ALSEC, que concreta como obligación del PSSIisc cualificado la de conservar la información relativa a los SSIisc cualificados por ellos prestados por un período de tiempo de quince años.

SSIisc cualificado, de acuerdo con las disposiciones verificadas por el organismo de supervisión con arreglo al artículo 17.4.i) RIE-SCTE; j) garantizar un tratamiento lícito de los datos personales, de conformidad con el RPPFTDP[854].

Este artículo 24 RIE-SCTE viene a corresponderse, en parte, con el contenido de los artículos 12, 13 y 20 LFE, todos ellos referidos solamente a obligaciones vinculadas con la expedición de certificados electrónicos reconocidos, no encontrándose prevista regulación similar alguna para el supuesto en que el PSSIic preste otros SSIic en relación con la firma electrónica.

Más específicamente, el primero de los preceptos regula una serie de obligaciones previas a la expedición de tales certificados, coincidiendo tan sólo la primera de las letras con el contenido del correspondiente y posterior artículo 24.1 RIE-SCTE; de acuerdo con el mismo, antes de la expedición del ahora denominado certificado electrónico cualificado, los PSSIisc cualificados deberán cumplir las siguientes obligaciones:

> «a) Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente[855].
>
> b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
>
> c) Asegurarse de que el firmante tiene el control exclusivo sobre el uso de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
>
> d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación».

El incumplimiento por el PSSIisc de las obligaciones contenidas en las letras b) a d) al garantizar un certificado electrónico expedido por un PSSIisc establecido en un Estado no

[854] Que, como sabemos, deroga a la DPPFTDP, que es la que aparece, por ser la vigente en el momento de su entrada en vigor, en el texto del Reglamento eIDAS.

[855] Esta comprobación, de acuerdo con el artículo 13.5 LFE y en línea con el actual artículo 24.1.2º RIE-SCTE, podrá realizarse personalmente por el PSSIisc cualificado o por medio de otras personas, físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el citado PSSIisc.

perteneciente al EEE determinará la responsabilidad de aquel por los daños y perjuicios causados por el uso de dicho certificado (artículo 22.2 LFE).

Como desarrollo de la letra a) anterior nace el artículo 13 LFE, que, adaptado al lenguaje propiciado por la nueva regulación comunitaria, distingue dos supuestos, uno para personas físicas y otro para personas jurídicas. Por lo que respecta al primero, dispone que la identificación de la persona física que solicite un certificado electrónico cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el DNI, pasaporte u otros medios admitidos en Derecho; en su defecto, podrá prescindirse de esta personación si la firma del solicitante del certificado electrónico ha sido legitimada en presencia notarial. Además, añade, cuando los certificados sean expedidos previa identificación del solicitante ante las Administraciones públicas, el régimen de personación se regirá por lo establecido en la normativa administrativa.

En el caso de personas jurídicas, se exige la comprobación adicional por los PSSIisc cualificados de «[…] los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible»; esta comprobación podrá realizarse, también, mediante consulta en el registro público en el que se hallen inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por tales registros. Si el certificado electrónico cualificado refleja una relación de representación voluntaria, el PSSIisc cualificado deberá comprobar los datos relativos a la personalidad jurídica del representado y a la extensión y vigencia de las facultades del representante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible, existiendo, aquí también, la posibilidad de realizar la comprobación consultando en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros; asimismo, si el certificado electrónico admite otro supuesto de representación, será necesaria, en la misma forma antes descrita, la acreditación por el PSSIisc de las circunstancias en que se fundamenten. Por último, caso de que dicho certificado contenga otras circunstancias personales o atributos del solicitante (condición de titular de un cargo público, pertenencia a un colegio profesional o titulación), estas deberán ser comprobadas a través de los documentos oficiales que las acrediten, de acuerdo con su normativa específica.

Ahora bien, lo antes dispuesto para personas físicas y jurídicas no será exigible en dos casos concretos: a) cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al PSSIisc en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación fuese menor a cinco años, y b) cuando para solicitar un certificado electrónico se utilice otro vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este precepto y le conste al PSSIisc que el período de tiempo transcurrido desde la identificación es menor a cinco años.

Por último, el artículo 20 LFE incluye obligaciones varias que, tras la entrada en vigor del Reglamento eIDAS, habrían de ubicarse, según el caso, en el apartado primero o segundo del artículo 24 RIE-SCTE. Este precepto, por entonces ceñido a la expedición de certificados electrónicos reconocidos, podría verse adaptado hasta el momento de su derogación por una redacción que podría ser similar a la que sigue:

*1. Además de las obligaciones establecidas en este capítulo, los prestadores cualificados de servicios de confianza que presten servicios de confianza cualificados deberán cumplir las siguientes obligaciones:*

*a) Demostrar la fiabilidad necesaria para prestar servicios de confianza*[856].

*b) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de confianza ofrecidos y los procedimientos de seguridad y de gestión adecuados en este ámbito*[857].

*c) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad y la fiabilidad técnicas de los procesos que sustentan*[858].

[856] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra a) del anexo II DFE y con la, igualmente derogada, letra b) del artículo 12 RDLFE. Esta letra no encontraría equivalente explícito en el actual artículo 24 RIE-SCTE.

[857] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra e) del anexo II DFE y con la, igualmente derogada, letra d) del artículo 12 RDLFE. También con la letra b) del actual artículo 24.2 RIE-SCTE.

[858] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra f) del anexo II DFE y con la, igualmente derogada, letra e) del artículo 12 RDLFE. También con la letra e) del actual artículo 24.2 RIE-SCTE.

*d) Tomar medidas contra la falsificación y el robo de datos y, en el caso de que el prestador de servicios de confianza genere datos de creación de firma o sello electrónicos, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante o al creador de un sello, respectivamente. Si el prestador de servicios de confianza gestiona los datos de creación de firma o sello electrónicos en nombre del firmante, deberá custodiarlos y protegerlos frente a cualquier alteración, destrucción o acceso no autorizado, así como garantizar su continua disponibilidad para el firmante o el creador de un sello, respectivamente* [859].

*e) Conservar registrada por cualquier medio seguro y posiblemente electrónico toda la información y documentación referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza y las declaraciones de prácticas de los servicios electrónicos de confianza vigentes en cada momento, al menos durante quince años contados desde el momento de su expedición, en particular al objeto de que sirvan de prueba en procedimientos legales y para garantizar la continuidad del servicio*[860].

*f) Utilizar sistemas fiables para almacenar los datos que se les faciliten de forma verificable, de modo que estén a disposición del público para su recuperación sólo cuando se haya obtenido el consentimiento de la persona a la que corresponden los datos, sólo personas autorizadas puedan hacer las anotaciones y modificaciones en los datos almacenados y pueda comprobarse la autenticidad de los datos*[861].

*2. Los prestadores cualificados de servicios de confianza que expidan certificados electrónicos cualificados deberán, además, garantizar que pueda determinarse con precisión la fecha y hora en las que se expidió un certificado electrónico o se extinguió o suspendió su vigencia*[862].

*3. Los prestadores de servicios de confianza que expidan certificados electrónicos cualificados deberán constituir un seguro de responsabilidad civil por importe de, al menos, 3.000.000 de euros para afrontar el riesgo de la*

[859] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra g) del anexo II DFE y con la, igualmente derogada, letra f) del artículo 12 RDLFE. También con la letra g) del actual artículo 24.2 RIE-SCTE.

[860] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra i) del anexo II DFE y con la, igualmente derogada, letra h) del artículo 12 RDLFE. También con la letra h) del actual artículo 24.2 RIE-SCTE.

[861] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra l) del anexo II DFE y con la, igualmente derogada, letra j) del artículo 12 RDLFE. También con la letra f) del actual artículo 24.2 RIE-SCTE.

[862] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra c) del anexo II DFE y con la, igualmente derogada, letra a) del artículo 12 RDLFE. También, en cierto modo, con la letra k) del actual artículo 24.2 RIE-SCTE.

*responsabilidad por los daños y perjuicios que puedan ocasionar los servicios de confianza que presten. La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea de, al menos, 3.000.000 de euros. Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto*[863].

Estos tres preceptos quedarían encuadrados, caso de entrar en vigor, en los artículos 7 y 11.3.b) y e) ALSEC, que desarrollan las previsiones requeridas por el Reglamento eIDAS. Empezando por la última de las previsiones plasmadas en el propuesto precepto anterior, la letra b) del artículo 11.3 del Anteproyecto introduce dos novedades importantes: de una parte, reduce a la mitad la cuantía del seguro de responsabilidad civil, cuantía que (como ya hiciera el artículo 16.1 LFE) no será obligatoria si el PSSIisc pertenece al sector público; de otra, incorpora una posible elevación gradual de este importe, que se verá incrementado en 500.000,00 € por cada SSIisc cualificado que preste el PSSIisc cualificado. Por lo demás, se mantiene la posibilidad de sustituir, total o parcialmente, tal garantía por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea coherente con lo antes expuesto.

Por su parte, y sólo en relación con la expedición de certificados electrónicos cualificados, el artículo 11.3.d) ALSEC impone al PSSIisc cualificado la obligación de asegurarse de que el titular del certificado en cuestión «[…] puede controlar el acceso y uso de los datos de creación de firma o sello o de autenticación de sitio web correspondientes a los de verificación que consten en el certificado».

Finalmente, en relación con la comprobación de la identidad prevista en el artículo 24.1 RIE-SCTE, el artículo 7 ALSEC, sustituyendo al artículo 13 LFE, vendría a establecer lo siguiente:

«1. La identificación de la persona física que solicite un certificado cualificado exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación

[863] Esta letra vendría a corresponderse, con los matices oportunos, con la derogada letra h) del anexo II DFE y con la, igualmente derogada, letra g) del artículo 12 RDLFE. También con la letra c) del actual artículo 24.2 RIE-SCTE.

de la persona física que solicite un certificado cualificado si su firma en la solicitud de expedición de un certificado cualificado ha sido legitimada en presencia notarial.

2. Por Orden ministerial se podrán determinar las condiciones y requisitos aplicables a la verificación de la identidad y, si procede, otros atributos específicos de la persona solicitante de un certificado cualificado mediante otros medios de identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física.

3. En el caso de certificados cualificados de sello electrónico y de firma electrónica con atributo de representante, los prestadores de servicios de confianza comprobarán, además de los datos señalados en los apartados anteriores, los datos relativos a la constitución y personalidad jurídica y a la persona o entidad representada, respectivamente, así como la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente y su inscripción en el correspondiente registro público si así resulta exigible.

Esta comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

4. Cuando el certificado cualificado contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

5. Lo dispuesto en los apartados anteriores podrá no ser exigible en los siguientes casos:

a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de confianza en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b) Cuando para solicitar un certificado se utilice otro vigente para cuya expedición se hubiera identificado a la persona física solicitante en la forma prescrita en este artículo y le conste al prestador de servicios que el período de tiempo transcurrido desde la identificación es menor de cinco años.

La forma en que se ha procedido a identificar a la persona física solicitante podrá constar en el certificado. En otro caso, los prestadores de servicios deberán colaborar entre sí para determinar

cuándo se produjo la última personación o medio equivalente de identificación al que alude el apartado 2».

En séptimo lugar, el artículo 30 LFE añade, *específicamente para los PSSIic* (también para la actual entidad nacional de acreditación y para los organismos de certificación), la *obligación de colaboración específica*, al establecer el deber de comunicar al actual Ministerio de Energía, Turismo y Agenda Digital «[…] el inicio de su actividad, sus datos de identificación, incluyendo la identificación fiscal y registral, en su caso, los datos que permitan establecer comunicación con el prestador, incluidos el nombre de dominio de internet, los datos de atención al público, las características de los servicios que vayan a prestar, las certificaciones obtenidas para sus servicios y las certificaciones de los dispositivos que utilicen»; esta información habrá de ser convenientemente actualizada por los PSSIisc y será objeto de publicación en la dirección de Internet de dicho Ministerio con la finalidad de otorgarle la máxima difusión y conocimiento (artículo 30.2 LFE). En la actualidad, el artículo 20 ALSEC prevé la derogación del artículo 30 LFE, manteniendo una redacción similar salvo por la introducción de cuatro novedades importantes: a) la ampliación del elenco de sujetos obligados, al añadir a los organismos de evaluación de la conformidad y a todas aquellas personas o entidades relacionadas con el PSSIisc; b) la modificación del precepto de referencia de la LJCA, que pasa a ser el artículo 8.6; c) la reducción del ámbito de aplicación de la obligación de información contenida en el artículo 30.2 LFE únicamente a los PSSIisc cualificados, y d) la incorporación de una nueva obligación, también circunscrita a los PSSIisc, cual es la de remitir al Ministerio de Energía, Turismo y Agenda Digital (que es, en España, el organismo de supervisión –artículo 17 Reglamento eIDAS–), a más tardar el 1 de febrero de cada año, «[…] un informe sobre sus datos de actividad del año civil precedente, con objeto de cumplimiento por parte de éste de las obligaciones de información a la Comisión Europea» al amparo del artículo 17.6 RIESCTE.

Para concluir, y *como obligación propia*, en este caso, *de los PSSIisc no cualificados*, se encontraría eventualmente la previsión de la D. T. Única ALSEC, que establece el *deber de los PSSIisc no cualificados que ya vinieran prestando SSIisc no cualificados de comunicar su actividad* al Ministerio de Energía, Turismo y Agenda Digital en el plazo de tres meses desde la entrada en vigor del ahora Anteproyecto. Se exceptúan, aquí, «[…] aquellos que hubieran comunicado los servicios prestados al Ministerio de Energía, Turismo y Agenda Digital antes de la entrada en vigor de esta ley».

### 3.3. Régimen de responsabilidad

La Sección 2ª del Capítulo II del Título II (artículos 13 a 17) de la LSSICE regula el régimen de responsabilidad general del conjunto de PSSI. En lo que a efectos de este estudio interesa, el artículo 13 LSSICE, que no encuentra su homónimo en la DCE, dispone en su apartado primero que todos los PSSI estarán sujetos «[…] a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley». Ello significa que los PSSI sólo serán responsables por los contenidos que ellos mismos elaboren o que se hayan elaborados por cuenta suya[864], afirmación esta que resulta del todo superflua, habida cuenta de que no modifica en modo alguno el régimen jurídico de los sujetos afectados, limitándose a decir tautológicamente que quedarán afectados por las normas que les afecten; lo mismo sucede con el último inciso «[…] sin perjuicio de lo dispuesto en esta Ley», que nada añade en el plano de los efectos jurídicos[865]. No obstante, hay otros autores[866] que sostienen que, al establecer este apartado que todos los PSSI quedarán sujetos a diferentes tipos de responsabilidad sin perjuicio de lo dispuesto en esta norma, se está dando origen a una suerte de régimen de responsabilidad transversal y especial; esto significaría que el régimen de responsabilidad contenido en la LSSICE prevalecería sobre cualquier otro tipo de responsabilidad jurídica que, de un modo más genérico, pudiera resultar atribuible.

Partiendo de esta previsión conjunta, el apartado segundo del mismo precepto introduce una previsión general para los PSSIi que, recogida posteriormente por la normativa en materia de servicios de confianza para los PSSIisc, tendrá su reflejo actual en los artículos 22 y 23 LFE. De acuerdo con el artículo 13.2 LSSICE, para determinar la responsabilidad de los PSSIi se estará a lo establecido en los artículos siguientes, haciendo alusión con esta previsión a los artículos 14 a 17 de la Ley y olvidando, sin justificación alguna, a aquellos que prestan SSIisc.

En cualquier caso, a todos resulta evidente a estas alturas de la investigación que los PSSIisc forman parte del grupo más amplio de PSSIi, motivo por el cual se hace preciso

---

[864] PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, cit., p. 270.

[865] PEGUERA POCH, M., *Principios de Derecho de la sociedad de la información*, cit., p. 351.

[866] Entre otros, *vid.* PÉREZ BES, F., *El Derecho de Internet*, cit., p. 231.

acudir, en un primer estadio, al ya derogado artículo 22 DFE. Este precepto, sin perjuicio de cuanto se contuviera en la DCACCC, establecía la necesidad de que, como mínimo, el PSSIic que expidiese al público un certificado electrónico presentado como reconocido[867], fuese responsable, salvo que demostrase que no había actuado con negligencia (algo que entendemos extensible también al PSSIisc no reconocido), por el perjuicio causado a cualquier entidad o persona física o jurídica que confiase razonablemente en dicho certificado: en primer lugar, por lo que respecta a la veracidad, en el momento de su expedición, de toda la información contenida en el certificado electrónico en cuestión y la inclusión en el mismo de toda la información prescrita para aquellos que fuesen reconocidos; a la garantía de que, en el momento de la expedición del certificado electrónico, obraban en poder del firmante identificado en el mismo los datos de creación de firma electrónica correspondientes a los datos de verificación que en él constan o se identifican, y a la garantía de que los datos de creación y de verificación de firma electrónica podían utilizarse complementariamente, caso de que el PSSIic generase ambos. En segundo lugar, por no haber registrado la revocación del certificado electrónico. En cualquier caso, la mencionada Directiva otorgaba al PSSIic la posibilidad de consignar limitaciones concernientes a los posibles usos y al valor máximo de las transacciones a efectuar con el certificado reconocido, siempre y cuando estos fuesen reconocidos por terceros, quedando exonerado de responsabilidad alguna en relación con aquellos perjuicios que se deriven de la superación de estas delimitaciones.

Tras la aparición del Reglamento eIDAS, el artículo 13 DFE se ha visto reemplazado por el artículo 13 RIE-SCTE, que se aplicará con arreglo a las normas nacionales sobre responsabilidad. Este nuevo artículo, más adecuado por no estar centrado en la responsabilidad por la expedición de certificados electrónicos, ciertamente relevante pero no la única que llevan a cabo (ni antes ni ahora) los PSSIisc, viene a determinar la responsabilidad de los PSSIisc (cualificados y no cualificados, sin distinción, a diferencia de su homónimo anterior) por «[…] los perjuicios causados de forma deliberada o por negligencia a cualquier persona física o jurídica en razón del incumplimiento de las obligaciones establecidas en el presente Reglamento». Ahora bien, al igual que con la DFE, la carga de la prueba de que el PSSIic cualificado no ha actuado con negligencia rece sobre él mismo; en cambio, y como novedad no contenida en la normativa precedente, se invierte la carga de la prueba en aquellos supuestos en

[867] Aunque luego no lo fuese, dada la apariencia creada (CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, cit., pp. 66 y 67).

que el perjuicio causado se halle relacionado con un servicio proporcionado por un PSSIisc no cualificado, siendo la persona física o jurídica afectada quien halla de alegar el daño padecido. Entendemos justo el distinto tratamiento legal proporcionado si lo que se pretende es inferir un plus de seguridad jurídica a los usuarios de SSIisc cualificados, dado que esta es la finalidad fundamental que les lleva a contratarlos; no obstante, no podemos dejar de subrayar un hecho evidente, como es la mayor facilidad que, en principio, tendrá la persona que padezca el perjuicio para probarlo que la persona que alega no haberlo causado, dejando, en ocasiones, al PSSIisc cualificado en una manifiesta y poco justificable situación de indefensión. Por lo demás, y como ya hiciera la DFE, el Reglamento eIDAS establece excepciones a la responsabilidad de los PSSIisc (cualificados y no cualificados) siempre que, con anterioridad al momento del perjuicio y en lo que exceda de la previsión que se comunique, «[…] informe debidamente a sus clientes con antelación sobre las limitaciones de la utilización de los servicios que presta y estas limitaciones sean reconocibles para un tercero» (artículo 13.2 RIE-SCTE), por ejemplo, mediante su inclusión en las CGC del SSIisc prestado o por otros medios reconocibles (considerando 37 Reglamento eIDAS); empero, a diferencia de la Directiva, el Reglamento parece hablar tan sólo de limitaciones de uso y no de valor, aspecto que, de ser así, resultaría del todo inadecuado para los intereses del PSSIisc.

En nuestro país, la previsión del artículo 13 DFE dio lugar a los artículos 22 y 23 LFE, que, sustituyendo al artículo 14 RDLFE[868], regulan, sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores, los supuestos de incursión en responsabilidad y de limitaciones o excepciones a la misma, respectivamente. Si atendemos al primero de ellos, los PSSIisc (cualificados y no cualificados) responderán por los daños y perjuicios ocasionados a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone la LFE, siendo esta responsabilidad exigible de acuerdo con las normas generales sobre culpa contractual o extracontractual, según proceda; además, como ya hiciera la DFE de la que parte, atribuye la carga de la prueba al PSSIisc, sin distinción alguna en función de la cualificación o no cualificación de los SSIisc prestados

[868] Este artículo, muy similar al artículo 22 LFE, se diferenciaba, sin embargo, por la inclusión de una previsión que, por la gravedad que podría implicar, fue derogado con la nueva Ley; nos referimos al apartado 3, *in fine*, del artículo 14 RDLFE, que obligaba al PSSIic (reconocido o no reconocido) a responder de la deuda en la cuantía que, en su caso, excediera de la garantía constituida «[…] con todos sus bienes presentes y futuros».

(artículos 22.1.2º, *in fine*, y 23.6 LFE). En cualquier caso, los PSSIisc asumirán toda la responsabilidad frente a terceros por la actuación de las personas en quienes deleguen la ejecución de alguna/s de la/s funciones necesarias para la prestación de SSIisc.

No obstante lo anterior, en nada será responsable el PSSIisc por los daños y perjuicios ocasionados a terceros de buena fe o al firmante si este (que, entiendo, sería el responsable efectivo) incurre en alguno de los siguientes supuestos: a) no haber proporcionado al PSSIisc «[…] información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia», siempre que su inexactitud no haya podido ser detectada por el PSSIisc; b) no comunicar sin demora al PSSIisc cualquier modificación de las circunstancias reflejadas en el SSIisc, en particular las reflejadas en el certificado electrónico; c) incurrir en negligencia en la conservación de sus datos de creación de firma electrónica, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación de estos o, en su caso, de los medios que den acceso a ellos; d) no solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma electrónica o, en su caso, de los medios que den acceso a ellos; e) utilizar los datos de creación de firma electrónica una vez expirado el período de validez del certificado electrónico o con posterioridad al momento en el que el PSSIisc le notifique la extinción o suspensión de su vigencia, y f) superar los límites que figuren en el certificado electrónico en cuanto a las posibles limitaciones de la utilización de los SSIisc o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el PSSIisc (artículo 23.1 LFE). Caso de que el certificado electrónico contemple una relación de representación, tanto el firmante (representante) como el representado, siempre que este último tenga constancia de la existencia de dicho certificado, estarán obligados a solicitar la revocación o suspensión de su vigencia, en los términos previstos por la Ley; en estos casos, entiendo que, si ninguno de ellos lo solicita, ambos serán responsables (no se especifica en qué condición). Tampoco será responsable el PSSIisc por la actuación negligente de, en este caso, los destinatarios de los documentos firmados electrónicamente, conclusión que podremos extraer en dos posibles casos: a) cuando no compruebe ni tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a su utilización; b) cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicado en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica (artículo 23.4 LFE). Por último, tampoco será responsable en aquellos casos en que se produzca inexactitud en

los datos que consten en el certificado electrónico si estos proceden de un documento público, inscrito en un registro público si así resulta exigible; caso de que dichos datos deban constar en un registro público, el PSSIisc podrá, en su caso, comprobarlos en dicho registro antes de la expedición del certificado, «[…] pudiendo emplear los medios telemáticos facilitados por los citados registros públicos» (artículo 23.5 LFE); no se pronuncia la norma acerca de quién sería el responsable de los perjuicios causados en estos casos, aunque todo parece indicar que sería el encargado del registro público correspondiente.

Ahora bien, de quedar derogada la LFE en detrimento del ALSEC, los artículos 13 y 14 de esta última Ley vendrían a reemplazar los antes analizados, y lo harían en una línea muy similar a la ya existente. En efecto, de acuerdo con el Anteproyecto, los PSSIisc responderían por los daños y perjuicios causados, por sí mismos o por delegación en otros, a cualquier persona (física o jurídica, se deduce) en el ejercicio de su actividad cuando incumplan con las obligaciones que les impone esta norma y el RIE-SCTE. También se establecen supuestos de exoneración de responsabilidad que coinciden con los previstos en el artículo 23, apartados 1 –a excepción de la letra f)– y 4 –a excepción de la letra a)[869]–, LFE. No se establece ahora, sin embargo, el sujeto sobre el que recae la carga de la prueba, habiendo de estar a lo dispuesto en el artículo 13.1.2º y 3º Reglamento eIDAS.

### 3.4. Régimen de supervisión y control

De esta cuestión se ocupa, a nivel comunitario, el artículo 19.1 DCE. De acuerdo con este precepto, los Estados miembros estarán obligados a disponer de los medios de control e investigación necesarios para poder aplicar la presente Directiva de manera eficaz, garantizando que los PSSI comunican la información requerida.

En España, el artículo 35 LSSICE regula el control del cumplimiento de la actividad de los PSSI. Más específicamente, dispone su apartado primero que el Ministerio de Industria, Energía y Turismo[870] controlará el cumplimiento por los PSSI de las obligaciones establecidas en la LSSICE y en sus disposiciones de desarrollo en todo aquello que se refiera a los SSI. No obstante, incluye un párrafo segundo que precisa que las referencias efectuadas a los

[869] En cualquier caso, estas excepciones se entenderían cubiertas por lo establecido en el artículo 13.2 RIE-SCTE.

[870] En la actualidad, Ministro de Energía, Turismo y Agenda Digital.

órganos competentes en los preceptos 8, 10, 11, 15, 16, 17 y 38 LSSICE se entenderán realizadas a los órganos jurisdiccionales o administrativos que, en cada caso, lo sean en función de la materia. Para el ejercicio de la función de control que les corresponde, los órganos citados en el apartado anterior podrán realizar las actuaciones inspectoras precisas para el ejercicio de su función de control; los funcionarios que, adscritos a dichos órganos, ejerzan dicha inspección tendrán la consideración de autoridad pública en el desempeño de sus cometidos. En cualquier caso, pese a lo anterior, cuando las conductas realizadas por los PSSI «[…] estuvieran sujetas, por razón de la materia o del tipo de entidad de que se trate, a ámbitos competenciales, de tutela o de supervisión específicos, con independencia de que se lleven a cabo utilizando técnicas y medios telemáticos o electrónicos, los órganos a los que la legislación sectorial atribuya competencias de control, supervisión, inspección o tutela específica ejercerán las funciones que les correspondan» (artículo 35.3 LSSICE).

Paralelamente, en el ámbito concreto de los SSIisc, el artículo 29 LFE viene a establecer que también el actual Ministerio de Energía, Turismo y Agenda Digital controlará el cumplimiento por los PSSIisc que presten SSIisc (redacción actualizada como consecuencia de la entrada en vigor del RIE-SCTE) de las obligaciones establecidas en la norma y en sus disposiciones de desarrollo. De igual modo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica. Para el ejercicio de dicha función de control, tal Ministerio realizará las actuaciones inspectoras que sean precisas, teniendo, a tal efecto, la consideración de autoridad pública en el desempeño de sus cometidos. Asimismo, podrá acordar las medidas que se estimen apropiadas para el cumplimiento de la Ley y de sus disposiciones de desarrollo, pudiendo, de un lado, recurrir a entidades independientes y técnicamente cualificadas para que le asistan en las labores de supervisión y control sobre tales PSSIisc, y, de otro, requerir la realización de pruebas en laboratorios o entidades especializadas para acreditar el cumplimiento de determinados requisitos, corriendo, en este caso, los PSSIisc con los gastos ocasionados por la evaluación.

Este artículo vendría a bifurcarse en dos de entrar en vigor finalmente el ALSEC. En efecto, los artículos 17 y 18 del Anteproyecto vendrían a suplir el contenido del artículo 29 LFE. No se producen modificaciones sustanciales, si bien es cierto que se explicitan las medidas que el Ministerio de Energía, Turismo y Agenda Digital, como órgano de supervisión, podrá adoptar para controlar el cumplimiento por los PSSIisc (cualificados y no cualificados) que ofrezcan SSIisc al público de las obligaciones establecidas en el Reglamento eIDAS y en

el propio ALSEC. En este sentido, dispone el artículo 17.2.2º ALSEC que el citado Ministerio podrá dictar directrices para la elaboración y comunicación de informes y documentos y para el cumplimiento de las obligaciones técnicas y de seguridad exigibles a los SSIisc, así como sobre requisitos y normas técnicas de auditoría y certificación con arreglo a las cuales los organismos de evaluación de la conformidad realizarán la evaluación de la conformidad de los PSSIisc cualificados; para ello, se podrán referenciar especificaciones o normas elaboradas por la ENISA o por organismos de estandarización europeos e internacionales.

### 3.5. Régimen de infracciones y sanciones

Los PSSIisc que presten SSIisc relacionados con la firma electrónica se verán sujetos, en primer lugar, al régimen general de infracciones y sanciones establecido en el artículo 20 DCE[871] y en el Título VII (artículos 37 a 45) LSSICE en aquello que les resulte de aplicación, y, en segundo lugar, al régimen específico contemplado actualmente en el artículo 16 RIESCTE[872] y en el Título VI (artículos 31 a 36) LFE, este último pendiente de ser derogado, quién sabe si en favor del Título V (artículos 21 a 23) ALSEC (**anexo XXX**).

#### 3.5.1. Afectados

De acuerdo con el artículo 37 LSSICE, todo aquel PSSI (incluidos, pues, los PSSIi) que incurra en alguna de las infracciones, muy graves, graves o leves, previstas en el artículo 38 LSSICE, estará sujeto al régimen sancionador establecido en el Título VII de la norma. Carece de una previsión similar el Título VI LFE, que pasa directamente a regular las concretas sanciones en que pueden incurrir los actuales PSSIisc; lo mismo sucederá con el Título V ALSEC.

---

[871] «Los Estados miembros determinarán las sanciones aplicables a las infracciones de las disposiciones nacionales que se adopten en aplicación de la presente Directiva y tomarán todas las medidas necesarias para garantizar su aplicación. Las sanciones que establezcan deberán ser efectivas, proporcionadas y disuasorias». A este artículo se acompaña el considerando 54 DCE, que aclara que las sanciones que se impongan al amparo de esta norma se entenderán sin perjuicio de cualquier otra sanción o reparación que pudiera establecerse en la legislación propia de los distintos Estados miembros, a la vez que añade que tales Estados miembros no estarán obligados a establecer sanciones de orden penal por la infracción de las disposiciones nacionales adoptadas en aplicación de la presente DCE.

[872] «Los Estados miembros establecerán normas relativas a las sanciones aplicables a las infracciones del presente Reglamento. Las sanciones previstas serán eficaces, proporcionadas y disuasorias».

Por lo demás, las sanciones que se impongan deberán satisfacer una triple exigencia: habrán de ser efectivas, proporcionadas y disuasorias (artículos 20 DCE y 16 RIE-SCTE).

### 3.5.2. Supuestos

Recogidas íntegramente en los artículos 38 LSSICE y 31 LFE/21 ALSEC, las infracciones previstas en la normativa y en que pudieran incurrir los PSSIisc (cualificados o no cualificados) que presten SSIisc en materia de firma electrónica pueden clasificarse en muy graves, graves y leves.

Por lo que respecta a las *infracciones muy graves*, hemos de aludir, en primer lugar, a la contemplada en el artículo 38.2.b) LSSICE para PSSIi –los apartados a), c) y d) han sido derogados–. En este caso, entendemos que, aun cuando no alude expresamente a los PSSIisc, sí que su contenido sería plenamente aplicable, gracias a la previsión en él contenida, en la que habla de «[…] la prestación de cualquier otro servicio equivalente de intermediación». En concreto, señala este precepto que será infracción muy grave «[e]l incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red *o la prestación de cualquier otro servicio equivalente de intermediación*, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11»[873]. En mi opinión, una redacción más adecuada, o, cuanto menos, más acorde a los efectos inclusivos que ahora nos interesan, hubiera podido ser como sigue: *tendrá la consideración de infracción muy grave el incumplimiento de la obligación de suspender la prestación de cualquier actividad de intermediación, cuando un órgano administrativo competente lo ordene, en virtud de lo dispuesto en el artículo 11*.

En segundo lugar, tenemos que acudir, para analizar qué afecta específicamente a los PSSIisc, al artículo 31.2 LFE, que establece que serán infracciones muy graves las siguientes: a) el incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 LFE

[873] La cursiva es propia.

en la prestación de SSI cualificados[874], siempre que se hayan causado daños graves a los usuarios o la seguridad de los SSIisc[875] se haya visto gravemente afectada, excluyéndose, no obstante, el incumplimiento de la obligación de constitución de la garantía económica prevista en el artículo 20.2 LFE, y b) la expedición de certificados electrónicos cualificados sin realizar todas las comprobaciones previas señaladas en el artículo 12 LFE, cuando ello afecte a la mayoría de los certificados electrónicos cualificados expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del PSSIisc cualificado, si este período es menor.

De ser derogada la LFE, el artículo 31.2 LFE dejaría de estar en vigor en detrimento, posiblemente, del artículo 21.2 ALSEC. Este precepto tan sólo prevé la conversión de una infracción grave en muy grave cuando, «[…] como consecuencia de ella, se hayan causado daños graves constatables a usuarios concretos o la seguridad de los servicios de confianza se haya visto gravemente afectada», es decir, la misma causa prevista en los artículos 31.2.a) y 31.3.d) LFE ante el incumplimiento de los artículos 18 y 20 LFE. La conclusión que cabría extraer de lo anterior es una más que manifiesta mitigación de la severidad de las sanciones a imponer a quienes resulten ser responsables de la infracción, sanciones que, salvo en muy reducidos casos, tendrán la consideración de muy graves; ello permitiría plantearnos una cuestión de no menor importancia, cual es la adecuación, o no, de esta decisión legislativa con las exigencias de eficacia, proporcionalidad y disuasión que, merced al artículo 16 RIE-SCTE, ha de perseguir toda sanción.

El plazo de prescripción para iniciar un proceso administrativo sancionador por infracciones muy graves será de tres años, mientras que las sanciones que se impongan por faltas de esta naturaleza prescribirán también a los tres años (artículo 45 LSSICE).

Atendiendo ahora a las *infracciones graves*, destacan, dentro del artículo 38.3.b) LSSICE, que afecta a todos los PSSI –el apartado a) ha sido derogado–, los siguientes apartados: b) y donde será calificado como tal el incumplimiento significativo de lo establecido en los párrafos a) (disponer de los medios que permitan, tanto a los DSSI como a los órganos competentes,

[874] Se sustituye aquí la redacción actual como consecuencia de la entrada en vigor del RIE-SCTE, en la que habla de las obligaciones establecidas «[…] en la expedición de certificados reconocidos».

[875] Se sustituye aquí la redacción actual como consecuencia de la entrada en vigor del RIE-SCTE, en la que habla de la seguridad «[…] de los servicios de certificación».

acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, al nombre o denominación social del PSSI; a su residencia o domicilio o, en su defecto, a la dirección de uno de sus establecimientos permanentes en España; a su dirección de correo electrónico y a cualquier otro dato que permita establecer con él una comunicación directa y efectiva) y f) (disponer de los medios que permitan, tanto a los DSSI como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, cuando el SSI haga referencia a precios, a información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, gastos de envío) del artículo 10.1 LSSICE; c) para el caso en el que el PSSIisc procediera como se indica, «[e]l envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, o su envío insistente o sistemático a un mismo destinatario del servicio cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21»[876] –artículo 38.3.c) LSSICE–; d) el incumplimiento significativo de la obligación del PSSI establecida en el apartado primero del precepto anterior, en relación con los procedimientos para revocar el consentimiento prestado por los DSSI –artículo 38.3.d) LSSICE–; e) no poner a disposición del DSSI las CGC a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27 LSSICE; f) el incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando se haya pactado su exclusión o el contrato se haya celebrado con un consumidor; g) la resistencia, excusa o negativa a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a la LSSICE; h) el incumplimiento significativo de lo establecido en el artículo 10.3 LSSICE, y, por último, i) la reincidencia en la comisión

[876] Conviene destacar cómo la AEPD ha venido sancionando como infracciones del artículo 21 LSSICE (graves o leves, según el caso) las ocasionadas por sistemas ideados para eludir la exigencia de consentimiento previo del DSSI, como sucede en aquellos casos en los que personas vinculadas con el anunciante proceden al reenvío de mensajes comerciales o aquellos otros en los que, desde la página web, se da la opción a sus clientes de recomendar un producto a personas por ellos conocidas –PÉREZ BES, F., *El Derecho de Internet*, cit., p. 141–. La previsión de sanciones graves para estos supuestos no ha contentado a todos, ya que, aparte de constituir una materia que ya se encuentra regulada y protegida en la normativa sobre protección de datos, se ha llegado a sostener que, si se prohíbe el *spamming* en España, los avances tecnológicos acabarán posibilitando idénticas acciones desde países en los que sí está permitida esta actividad, disminuyendo de manera ostensible el volumen de desarrollo económico en nuestro país. Pese a ello, mi postura, en línea con la expresada por DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, cit., p. 258, se encuentra radicalmente en contra del *spamming*, más allá de la conveniencia de posibilitar el cumplimiento de unas leyes verdaderamente adaptadas a la realidad social del momento, pues sólo así se conferirá a los afectados la seguridad jurídica pretendida en un contexto tan cambiante como es el del comercio electrónico.

de la infracción leve prevista en la letra g) del artículo 38.4 LSSICE, cuando así se hubiera declarado por resolución firme dictada en los tres años inmediatamente anteriores a la apertura del procedimiento sancionador.

Por su parte, para los PSSIisc, el artículo 31.3 LFE, dispone que serán infracciones graves las que se enumeran a continuación: a) el incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 LFE en la prestación de SSI cualificados[877], excepto de la obligación de constitución de la garantía prevista en el artículo 20.2 LFE, cuando no constituya infracción muy grave[878]; b) la falta de constitución por los PSSIisc de la garantía económica contemplada en el artículo 20.2 LFE; c) la expedición de certificados electrónicos cualificados sin realizar todas las comprobaciones previas indicadas en el artículo 12 LFE, en los casos en que no constituya infracción muy grave; d) el incumplimiento por los PSSIisc de las obligaciones señaladas en el artículo 18 LFE, si se hubieran causado daños graves a los usuarios o la seguridad de los SSIisc[879] se hubiera visto gravemente afectada; e) el incumplimiento por los PSSIisc de las obligaciones establecidas en el artículo 21 LFE respecto al cese de actividad de los mismos o la producción de circunstancias que impidan la continuación de su actividad, cuando las mismas no sean sancionables de conformidad con lo dispuesto en la LOPDCP[880]; f) la resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a la LFE o deficiente presentación de la información solicitada por parte del actual Ministerio de Energía, Turismo y Agenda Digital en su función de inspección y control, y g) el incumplimiento de las resoluciones dictadas por el precitado Ministerio para asegurar que el PSSIisc se ajuste a la LFE.

[877] Se sustituye aquí la redacción actual como consecuencia de la entrada en vigor del RIE-SCTE, en la que habla de las obligaciones establecidas «[…] en la expedición de certificados reconocidos».

[878] A la vista de los artículos 31.2.a).2º y 31.3.a), ambos de la LFE, no queda del todo claro si el supuesto del artículo 20.2 LFE puede ser objeto de infracción muy grave o no.

[879] Se sustituye aquí la redacción actual como consecuencia de la entrada en vigor del RIE-SCTE, en la que habla de la seguridad «[…] de los servicios de certificación».

[880] En la actualidad, y tras su entrada en vigor, deberemos compatibilizar esta previsión con el contenido del RPPFTDP.

Si finalmente entra en vigor el ALSEC, su artículo 21.3 establecería como infracciones graves las que siguen: a) la resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta Ley; b) el incumplimiento de un requerimiento de subsanación de una deficiencia constitutiva de infracción cuando éste haya tenido que dictarse por segunda vez; c) actuar en el mercado como PSSIisc cualificado, ofrecer SSIisc como cualificados o utilizar la etiqueta de confianza «UE» como PSSIisc cualificado sin haber obtenido la cualificación de los citados servicios; d) en caso de que el PSSIisc expida certificados electrónicos, almacenar o copiar, por sí o a través de un tercero, los datos de creación de firma electrónica o de sello electrónico de la persona física o jurídica a la que hayan prestado sus SSIisc, salvo en caso de su gestión en nombre del firmante o del creador del sello, respectivamente; e) no proteger adecuadamente los datos de creación de firma electrónica o de sello electrónico cuya gestión se le haya encomendado en la forma establecida en el artículo 11.2.a) ALSEC; f) no notificar, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de ellas, al Ministerio de Energía, Turismo y Agenda Digital cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el SSIisc prestado, salvo que sólo afecte a los datos personales tratados por el PSSIisc, o no ampliar la información notificada, según lo dispuesto en el artículo 16.3 ALSEC; g) cuando la violación de la seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el SSIisc, no notificar también a la persona física o jurídica, sin demora indebida, la violación de la seguridad o la pérdida de integridad; h) en caso de PSSIisc cualificados, el incumplimiento de alguna de las obligaciones establecidas en los artículos 24.2.b) a h) y k), 24.3 y 24.4 RIE-SCTE, con las precisiones establecidas, en su caso, por esta Ley, cuando no constituya infracción muy grave y no haya dado lugar a la retirada de la cualificación del PSSIisc; i) la expedición de certificados electrónicos cualificados sin realizar todas las comprobaciones previas relativas a la identidad u otras circunstancias del titular del certificado, o al poder de representación de quien lo solicita en su nombre, señaladas en el RIE-SCTE, y en esta Ley, u omitir la comprobación indicada en el artículo 11.3.d) ALSEC, cuando ello afecte a la mayoría de los certificados electrónicos cualificados expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del PSSIisc, si este período es menor, y j) no resolver los incidentes de seguridad en las redes y sistemas de información.

Las infracciones graves prescribirán a los dos años, al igual que las sanciones que se impongan por faltas de esta naturaleza (artículo 45 LSSICE).

En lo atinente, por último, a las *infracciones de naturaleza leve*, en primer lugar, sostiene el artículo 38.4 LSSICE un elenco que, a los efectos que aquí nos interesan, quedaría reducido al siguiente: b) no informar, en la forma prescrita por el artículo 10.1 LSSICE, sobre los aspectos señalados en las letras b), c), d), e) y g) de dicho precepto, o en las letras a) y f) cuando no constituya infracción grave; c) el incumplimiento de lo previsto en el artículo 20 LSSICE para las comunicaciones comerciales, ofertas promocionales y concursos; d) el envío de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 LSSICE y no constituya infracción grave; e) no facilitar la información a que se refiere el artículo 27.1 LSSICE, cuando las partes no hayan pactado su exclusión o el DSSI sea un consumidor; f) el incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28 LSSICE, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave; g) utilizar dispositivos de almacenamiento y recuperación de datos, cuando no se hubiera facilitado la información u obtenido el consentimiento del DSSI en los términos exigidos en el artículo 22.2 LSSICE; h) el incumplimiento de la obligación del PSSI establecida en el artículo 22.1 LSSICE, en relación con los procedimientos para revocar el consentimiento prestado por los DSSI, cuando no constituya infracción grave, y, por último, i) el incumplimiento de lo establecido en el artículo 10.3 LSSICE, cuando no constituya infracción grave.

Por otro lado, en segundo lugar, el artículo 31.4 LFE contempla un doble supuesto de infracciones leves para los PSSIisc. El primero consistente en el incumplimiento por estos de las obligaciones establecidas en el artículo 18 LFE, cuando no sea infracción grave. El segundo, a modo de cajón de sastre, en el incumplimiento por los PSSI de las restantes obligaciones recogidas en la LFE y ya analizadas anteriormente en el presente capítulo de esta obra, siempre que no constituyan infracción grave o muy grave, con la excepción de las obligaciones recogida en el artículo 30.2 LFE.

Si el artículo 31.4 LFE se viera derogado en favor del artículo 21.4 ALSEC, las infracciones leves pasarían a ser las siguientes: a) no publicar información veraz y acorde con esta Ley y con el RIE-SCTE; b) no comunicar el inicio de actividad, su modificación o cese por los

PSSIisc no cualificados en el plazo establecido en el artículo 15 ALSEC; c) el incumplimiento por los PSSIisc de alguna de las obligaciones establecidas en el artículo 24.2.a) e i) RIE-SCTE; d) no colaborar con otros PSSIisc cualificados para determinar la fecha, bien de la última personación de la persona física firmante o solicitante del sello, bien de empleo de un medio equivalente de identificación aceptado, cuando su colaboración sea necesaria; e) en caso de PSSIisc que expidan certificados electrónicos cualificados de sello electrónico, no registrar la información a la que se refiere el artículo 11.3.a) ALSEC, y f) el incumplimiento por los PSSIisc cualificados de su obligación de remitir un informe anual de actividad al Ministerio de Energía, Turismo y Agenda Digital antes del 1 de febrero de cada año.

El plazo establecido para iniciar un procedimiento sancionador por infracciones leves prescribirá a los seis meses; en cambio, las sanciones impuestas por faltas leves prescribirán al año (artículo 45 LSSICE).

### 3.5.3. Imposición

Resultado de la comisión de las infracciones previstas en el punto anterior, los artículos 39 LSSICE y 32 LFE (y, en su caso, el artículo 22 ALSEC) prevén una serie de sanciones proporcionalmente equivalentes a la gravedad de aquellas y que, como establecen los artículos 20 DCE y 16 RIE-SCTE, deberán ser eficaces, proporcionadas y disuasorias.

Por lo que respecta a la potestad sancionadora[881], de acuerdo con los dos primeros artículos anteriores, la comisión de infracciones muy graves conllevará la imposición de una multa que oscilará entre los 150.001,00 € y los 600.000,00 €; no obstante, la reiteración en un intervalo de tres años de dos o más infracciones de esta naturaleza, sancionadas con carácter firme, tendrán como posible resultado, en función de las circunstancias del caso, una sanción consistente en la prohibición de actuar en España durante un plazo máximo de dos años de duración[882]. En todo caso, y por lo que respecta a la LSSICE, teniendo en cuenta que, como consecuencia de las derogaciones efectuadas en el artículo 38.2 LSSICE, sólo se prevé en la actualidad una sanción muy grave y que el artículo 39.1.a).2º exige que, para que se imponga

[881] Que deberá ejercerse de conformidad con lo establecido en la LPACAP y en su normativa de desarrollo (actualizado, artículos 43.2 LSSICE y 36.2 LFE).

[882] Esta sanción, entiendo, será extensible a todo PSSI, con independencia de dónde se halle establecido, sea en España, fuera de España pero dentro de la UE o del EEE o fuera de la UE o el EEE.

la sanción de prohibición de actuación en España durante un plazo máximo de dos años, es necesaria la reiteración en el plazo de tres años de dos o más infracciones así consideradas, entiendo que el artículo 39.1.a).2º LSSICE no resultaría ya de aplicación.

Menor será, lógicamente, la cuantía de la multa que haya de recaer sobre quienes resulten responsables de una infracción calificada como grave, que ascenderá a un importe de entre 30.001,00 € y 150.000,00 € –artículos 39.1.b) LSSICE y 32.1.b) LFE–. Las infracciones graves y muy graves podrán llevar aparejada, a costa del sancionado, la publicación de la resolución sancionadora en el BOE y en dos periódicos de difusión nacional o en la página de inicio del sitio de Internet del PSSIisc y, en su caso, en el sitio de internet del Ministerio de Energía, Turismo y Agenda Digital, una vez que aquélla tenga carácter firme; para la imposición de esta sanción, se considerará la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito (artículos 39.2 LSSICE y 32.2 LFE).

Por último, quienes cometan una infracción de naturaleza leve serán sancionados con una multa de hasta 30.000,00 €[883] –artículos 39.1.c) LSSICE y 32.1.c) LFE–. El artículo 39 LSSICE concluye con un apartado tercero de dudosa redacción, toda vez que, excluyendo el supuesto en el que las sanciones sean impuestas a PSSI establecidos en España o fuera de nuestro país pero dentro de las fronteras de la UE o del EEE, contempla tan sólo el supuesto de PSSI establecidos fuera de dichos territorios para afirmar que, en estos casos, el órgano que hubiera impuesto la respectiva sanción podrá ordenar a los PSSIi (se deduce, establecidos en España) que tomen las medidas que resulten necesarias para impedir el acceso desde España a los SSI ofrecidos por aquellos; de este modo, al menos aparentemente, aquellos PSSI no afectados por esta previsión se verán beneficiados en perjuicio de quienes sí se encuentran incluidos dentro del ámbito de aplicación del artículo 39.3 LSSICE, medida esta que, de ser adoptada, tendría una vigencia máxima de dos años para las infracciones muy graves, de un año para las infracciones graves y de seis meses para las infracciones leves.

Con el ALSEC se prevé, en cambio, una modificación de estos intervalos, que serían de entre 150.001,00 € y 300.000,00 € por la comisión de infracciones muy graves; de entre 50.001,00 € y 150.000,00 € por la comisión de infracciones graves, y de entre 5.000,00 € y 50.000,00 € por la comisión de infracciones leves (artículo 22.1 ALSEC). Se reduciría, pues, en esta tendencia "moderante", la cuantía máxima de las sanciones muy graves, si bien se

[883] No existe, por tanto, un importe mínimo en estos casos.

incrementaría la cuantía máxima de las sanciones graves y leves, además de establecerse un importe mínimo para estas últimas.

Las cuantías impuestas por la LSSICE podrán verse moderadas por el órgano sancionador en el sentido de aplicar la escala correspondiente a la clase de infracción inmediatamente inferior en gravedad a la que proceda (sanción grave en caso de sanción muy grave o sanción leve en caso de sanción grave) si concurre alguno de los siguientes supuestos (artículo 39 bis.1 LSSICE): a) cuando se aprecie una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho cometido como consecuencia de la concurrencia significativa de varios[884] de los criterios establecidos en el artículo 40 LSSICE; b) cuando la entidad infractora haya regularizado la situación irregular de forma diligente; c) cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción; d) cuando el infractor haya reconocido espontáneamente su culpabilidad, o e) cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso, no siendo imputable a la entidad absorbente. Cabe, incluso, la posibilidad de que se acuerde no iniciar el procedimiento sancionador si, atendida la naturaleza de los hechos cometidos y la concurrencia significativa de los criterios *supra* indicados, el órgano sancionador opta, en su lugar, por apercibir al sujeto responsable a fin de que, en el plazo que aquel determine, este acredite la adopción de las medidas correctoras que resulten pertinentes, procediendo de lo contrario, ahora sí, la apertura del procedimiento sancionador derivado de dicho incumplimiento; para que esta circunstancia pueda producirse, será necesario que los hechos sean constitutivos de infracción leve o grave (nunca muy grave) conforme a lo dispuesto en la LSSICE y que el órgano competente no hubiera sancionado o apercibido con anterioridad al infractor por la comisión de infracciones (se entiende, dado el silencio de la norma, muy graves, graves o leves) previstas en esta Ley (artículo 39 bis.2 LSSICE).

En cualquier caso, en virtud de ambas normas (artículos 40 LSSICE y 33 LFE), la cuantía de las multas que se impongan, dentro de los límites indicados, se graduará atendiendo a los siguientes criterios: a) la existencia, o no, de intencionalidad; b) la reincidencia derivada de la comisión de infracciones de la misma naturaleza, cuando así se haya declarado por resolución firme; c) la naturaleza y la cuantía de los perjuicios causados; d) los beneficios obtenidos por

[884] Concepto, este, jurídicamente indeterminado, ya que no indica en qué casos dicha concurrencia es *significativa* ni qué número mínimo de estos criterios permitiría alcanzar la consideración *varios*.

la comisión de la infracción, y e) el volumen de facturación a que afecte la infracción cometida[885]. A ellas, la LSSICE añade dos más no contempladas en la LFE: a) el plazo de tiempo durante el que se haya venido cometiendo la infracción y b) la adhesión a un código de conducta o a un sistema de autorregulación publicitaria aplicable respecto a la infracción cometida, que cumpla con lo dispuesto en el artículo 18 o en la D. F. 8ª, ambos de la LSSICE, y que haya sido informado favorablemente por el órgano u órganos competentes.

De este modo, de la lectura conjunta de los artículos 39 bis.1.a) LSSICE y 40 LSSICE y 33 LFE, podemos deducir que, caso de producirse la concurrencia significativa de varios de los criterios enunciados en este último precepto, no sólo se podrá descender en la escala relativa a la clase de infracciones, sino que, dentro de ella, podría interponerse una cuantía tanto menor a medida que dichos criterios (uno o varios, dependiendo de las circunstancias del caso) fueran favorables al sancionado[886].

En el ALSEC (artículo 22.2), en cambio, se introduce un mayor número de posibles causas de graduación de las sanciones, a saber: a) el grado de culpabilidad o la existencia de intencionalidad; b) la continuidad o persistencia en la conducta infractora; c) la naturaleza y cuantía de los perjuicios causados; d) la reincidencia, por comisión en el término de un año de más de una infracción de la misma naturaleza, cuando así haya sido declarado por resolución firme en vía administrativa; e) el volumen de la facturación del PSSIisc responsable; f) el número de personas afectadas por la infracción; g) la gravedad del riesgo generado por la conducta o la persistencia del mismo, y h) las acciones realizadas por el PSSIisc encaminadas a paliar los efectos o consecuencias de la infracción.

---

[885] Como podemos observar, las letras d) y e) se hallan estrechamente relacionadas entre sí, ya que el beneficio obtenido por la comisión de la infracción será tanto mayor cuanto mayor sea el volumen de facturación a que afecte la infracción cometida. En este sentido, me parece acertada la postura manifestada al respecto por *Ibid.*, p. 268, quien aplaude esta medida por entender que, de no haberse recogido normativamente, se podrían producir situaciones en las que la cuantía de la multa resultase una inversión rentable para los infractores, atendiendo a los beneficios obtenidos con su actuación, pudiendo representar tal previsión legal «[…] la aplicación de un principio de proporcionalidad que haga pensar a algunos si merece la pena realizar determinadas acciones».

[886] No podemos olvidar que estos criterios son, en última instancia, un reflejo de la propia actuación del interesado en relación con la infracción por él cometida.

En cualquier caso, conviene tener presente que, en aquellos procedimientos sancionadores en que se diriman supuestos de infracciones graves o muy graves, podrán adoptarse medidas de carácter provisional y proporcional con los objetivos que se pretendan alcanzar en cada supuesto (artículos 41 LSSICE y 34 LFE, no previendo nada al respecto el ALSEC, de lo que cabría extraer la imposibilidad de implementar este tipo de medidas en el caso de que este Anteproyecto entrara finalmente en vigor). Estas medidas, previstas en la actualidad en la LPACAP[887] y en sus normas de desarrollo, podrán adoptarse siempre que se estimen necesarias para: en primer lugar, asegurar la eficacia de la resolución que definitivamente se dicte; en segundo lugar, garantizar el buen fin del procedimiento; en tercer lugar, evitar el mantenimiento de los efectos de la infracción, y, en cuarto y último lugar, procurar la defensa de los intereses generales. En particular, y en lo que aquí nos interesa, podrán acordarse las siguientes medidas provisionales: a) la suspensión temporal de la actividad del PSSIisc y, en su caso, el cierre provisional de sus establecimientos; b) el precinto, depósito o incautación de registros, soportes y archivos informáticos y de documentos en general, así como de aparatos y equipos informáticos de todo tipo, y c) la advertencia al público de la existencia de posibles conductas infractoras y de la incoación del expediente sancionador de que se trate, así como de las medidas adoptadas para el cese de dichas conductas. En la adopción y cumplimiento de estas medidas provisionales se respetarán, en cualquier caso, las garantías, normas y procedimientos contemplados en nuestro ordenamiento jurídico y dirigidos a proteger, cuando pudieran resultar afectados, los derechos a la intimidad personal y familiar (esta última, sólo prevista en la LSSICE, si bien, por extensión, se entiende también aplicable a los PSSIisc), a la protección de los datos personales, a la libertad de expresión (sólo prevista en la LSSICE, si bien, por extensión, se entiende también aplicable a los PSSIisc) o a la libertad de información (sólo prevista en la LSSICE, si bien, por extensión, se entiende también aplicable a los PSSIisc); ahora bien, añade el artículo 41.2.2º LSSICE, en aquellos casos en que la CE, las normas reguladoras de los respectivos derechos y libertades o las que resulten aplicables a las diferentes materias atribuyan competencia a los órganos jurisdiccionales para

[887] Concretamente, artículo 56 LPACAP, en cuyo apartado tercero se hace una remisión al elenco de medidas provisionales contenido en la LECiv. En los artículos 41 LSSICE y 34 LFE aún aparece la regulación anterior, contenida en la LRJAP-PAC, que, como sabemos, ha sido ya derogada en favor de la LPACAP.

intervenir en el ejercicio de actividades o derechos, únicamente la autoridad judicial competente podrá adoptar las medidas de carácter provisional descritas[888]. En todo caso, ante supuestos de urgencia que así lo justifiquen y con el objeto de proteger de manera inmediata aquellos intereses que estén en juego, estas medidas provisionales podrán ser acordadas con anterioridad a la iniciación del expediente sancionador, si bien deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, acuerdo que deberá tener lugar dentro de los quince días siguientes a su adopción y que podrá ser objeto del recurso que proceda; en cualquier caso, estas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o si el acuerdo de iniciación no contiene un pronunciamiento expreso acerca de las mismas (artículos 41.4 LSSICE y 34.4 LFE). Finalmente, añade el artículo 34.2 LFE una importante previsión que, a diferencia de lo que sucedía en aquellos casos en que un aspecto era recogido en la norma general (LSSICE) y no en la norma específica (LFE), habremos de entender sólo aplicable a los PSSIisc: estamos hablando de aquella que establece que, en los supuestos de daños de excepcional gravedad en la seguridad de los sistemas empleados por el PSSIisc que menoscaben seriamente la confianza de los usuarios en los SSIisc ofrecidos, el actual Ministerio de Energía, Turismo y Agenda Digital podrá acordar la suspensión o pérdida de vigencia de los SSIisc[889] afectados, «[…] incluso con carácter definitivo».

De no cumplirse en plazo las medidas provisionales acordadas, el órgano administrativo competente para resolver el procedimiento sancionador[890] podrá imponer multas coercitivas

---

[888] Como bien señala PEGUERA POCH, M., *Principios de Derecho de la sociedad de la información*, cit., p. 375, la declaración equivalente contenida en el artículo 8.1.3º LSSICE fue modificada por el artículo 4.2 LMISI, en el sentido de referir esa limitación de competencias de los órganos administrativos únicamente a los casos en que los tribunales tengan atribuida la competencia *de forma excluyente*; probablemente, añade el autor, no haber procedido en los mismos términos respecto del artículo 41.2.2º LSSICE deba atribuirse a un descuido del legislador.

[889] Se sustituye la redacción vigente en la LFE, donde se hablaba de *certificados*, como consecuencia de la entrada en vigor del RIE-SCTE, motivación esta que se añade, no obstante, a las dudas ya existentes anteriormente (y tantas veces apuntadas) sobre lo acertado de la previsión, que excluye la posibilidad, recogida en la definición de PSSIic contemplada en la LFE, de que este sujeto pueda llevar a cabo otra actividad que no sea la de expedición de certificados electrónicos (recuerden, «[s]e denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica»).

[890] En la actualidad, el Ministro de Energía, Turismo y Agenda Digital sería el órgano competente para las infracciones de naturaleza muy grave, mientras que el Secretario de Estado para la Sociedad de la Información

por importe máximo de 6.000,00 €[891] por cada día que transcurra sin proceder a dicho cumplimiento (artículos 42 LSSICE y 35 LFE).

Concluye la LSSICE (artículo 44, aplicable, por extensión, a los PSSIisc, aun cuando la LFE –ni el ALSEC– digan nada al respecto) el apartado relativo a la potestad sancionadora añadiendo que esta no podrá ejercerse si, con anterioridad, ha recaído ya sanción pena, siempre que se advierta identidad de sujeto, de hecho y de fundamento[892]. Si, en cambio, el proceso penal se está tramitando en el momento de la infracción regulada en la LSSICE y este tiene por objeto los mismos hechos u otros cuya separación de los sancionables con arreglo a esta última Ley es racionalmente imposible, el procedimiento quedará suspendido respecto de los mismos hasta tanto recaiga pronunciamiento firme de la autoridad judicial; reanudado el expediente, en su caso, la resolución que se dicte deberá respetar, como es lógico, los hechos declarados probados en dicha resolución judicial (artículo 44.1 LSSICE). Por otro lado, el hecho de que recaiga una sanción de las previstas en la LSSICE no impedirá que se pueda tramitar y resolver otro procedimiento sancionador tipificado en otra ley por los órganos u organismos competentes cuando, de un lado, la conducta infractora se haya cometido utilizando técnicas y medios telemáticos o electrónicos y, de otro, no haya identidad del bien jurídico protegido (artículo 44.2 LSSICE). En cambio, no se podrá imponer sanción alguna por hechos constitutivos de infracción según la LSSICE cuando también lo sean de otra tipificada en la normativa sectorial a la que el PSSI esté sujeto y exista identidad del bien jurídico protegido; en este sentido, cuando en el curso de una actuación sancionadora, se

y la Agenda Digital lo sería para las infracciones graves y leves (artículos 43.1 LSSICE y 36.1 LFE, así como, de entrar finalmente en vigor, artículo 23 ALSEC). No obstante lo anterior, se establecen las siguientes excepciones: en primer lugar, para la imposición de sanciones por incumplimiento de las resoluciones dictadas por los órganos competentes en función de la materia o entidad de que se trate a que se refiere el artículo 38.2 b) LSSICE –también se incluye en la redacción la letra a), ya derogada–, la competencia corresponderá al órgano que dictó la resolución incumplida (artículo 43.1.1º LSSICE); en segundo lugar, para la imposición de sanciones por la comisión de las infracciones relacionadas con las comunicaciones comerciales, tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h), ambos de la LSSICE, la competencia recaerá sobre la Agencia de Española de Protección de Datos (artículo 43.1.1º LSSICE), y, en tercer lugar, para el incumplimiento de las obligaciones establecidas en el artículo 17 LFE, el órgano competente será la AEPD, con arreglo a lo establecido en la LOPDCP/RPPFTDP (artículo 36.1.2º LFE). Ninguna excepción contempla al respecto el ALSEC.

[891] No existe, por tanto, un importe mínimo en estos casos.

[892] Doctrina relativa al principio *non bis in idem*.

tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a aquellos órganos u organismos competentes para su supervisión y sanción (artículo 44.3 LSSICE).

# CONCLUSIONI

Alla luce di quanto esposto nei quattro capitoli che costituiscono la presente ricerca è possibile trarre una serie di conclusioni rilevanti indicate di seguito.

**I.** Lo sviluppo e la diffusione globale delle nuove tecnologie dell'informazione e della comunicazione hanno favorito il transito dalla passata *società industriale o post-industriale* alla *società dell'informazione*, un nuovo spazio caratterizzato dalla centralità e accessibilità di massa del sapere e dal predominio dell'interazione comunicativa in forma virtuale tramite ciò che chiamiamo *ciberspazio*. Al suo interno, la 'Rete di reti' svolgerà un ruolo determinante come elemento di slancio e trasmissione illimitata, globale e immediata dei dati trattati, superando l'iniziale EDI e la sua limitata portata.

Il progresso descritto avverrà in maniera definitiva con la creazione della *www* o *Web*, un nuovo sistema che cambia radicalmente il concetto di Internet e, dunque, della società dell'informazione. Come qualsiasi altro ramo dell'innovazione tecnologica, il Web non è statico, ma si evolve parallelamente alle scoperte informatiche. Possiamo, quindi, vedere come, nel corso della sua evoluzione, il Web ha attraversato diversi stadi di sviluppo e di partecipazione: parliamo di *Web 1.0*, di sola lettura, permette ad altri utenti di navigare, ma non di modificare il contenuto e di adattare il sito in alcun modo; il *Web 2.0*, utilizzato per rispondere alla crescente partecipazione degli utenti alla creazione del contenuto e allo sviluppo delle infrastrutture informatiche che rendono possibile tale intervento; il Web 3.0, diffuso e provvisto di maggior significato, per cui qualsiasi utente può trovare risposte alle sue domande in maniera più veloce e semplice grazie a una configurazione dell'informazione meglio definita, e, infine, il *Web 4.0*, che avrebbe bisogno della creazione di sistemi capaci di eguagliare il ragionamento umano con l'obiettivo principale di collegare persone e dispositivi affinché entrambi riescano a prendere decisioni di comune accordo.

Potremmo parlare addirittura di uno stadio superiore d'evoluzione, recentissimo, in cui gli stessi soggetti destinatari dell'informazione selezionano e assimilano in maniera autosufficiente l'enorme quantitativo di contenuti disponibili a distanza per, farli diventare conoscenza quali frutto del pensiero autonomo e riflessivo. Questa evoluzione ha portato qualche autore ad elaborare una distinzione terminologica tra *società dell'informazione* e società *del sapere*: la prima metterebbe a disposizione della popolazione l'accesso a un'informazione quantitativamente illimitata (visione esterna o obiettiva); mentre la seconda si dovrebbe circoscrivere all'utilizzo o al trattamento razionale che l'individuo ricava da questa informazione (visione interna o soggettiva).

**II.** Il cambiamento di paradigma che comporta il nuovo modello di società comporta una serie di problemi importanti che necessitano di risposte adeguate e coerenti con la sicurezza di cui i soggetti aventi diritti e obblighi, principalmente condizionati dalla rivoluzione tecnologica, hanno bisogno per muoversi con sufficiente sicurezza in un mondo virtuale sempre più partecipe della vita quotidiana. In questo modo, la regolamentazione della rete attraverso il Diritto (ovvero, l'influenza dello spazio digitale in ambito giuridico e viceversa) diventa necessaria dato il carattere particolare del mezzo tecnico impiegato ed esige la corretta combinazione tra Diritto *tradizionale* e un nuovo tipo di Diritto, necessari entrambi all'interno di un contesto globale caratterizzato dalla crescente diversità e dall'incremento degli interessi commerciali.

Ciò avrà un duplice effetto. Il primo comporterà una revisione del vecchio Diritto, con l'adozione di misure legislative che siano adeguate per rimediare a molte delle soluzioni proposte dal vecchio ordine legale, adattandole alla realtà giuridica attuale, ma rispettando, per quanto possibile, il principio di inalterabilità del Diritto preesistente. Il secondo, al contrario, cercherà di dare una risposta ai cambiamenti con una parallela apparizione e incorporazione di sistemi e settori finora sconosciuti; questi cambiamenti non riguarderanno la natura del rapporto, ma piuttosto la natura tecnica del mezzo utilizzato, in particolare il suo carattere internazionale, incorporeo e delocalizzato. Da tutto questo nasce una nuova disciplina, conosciuta come *informatica giuridica*, che, a sua volta, si dirama in due direzioni distinte: da un lato, *il Diritto dell'informatica*, incentrato ad analizzare e cercare di risolvere i problemi giuridici posti dall'informatica e dove, per la prima volta nella storia, il Diritto diventa dipendente da un'altra disciplina per poter regolare in maniera adeguata gli avvenimenti sociali; da un altro lato, l'informatica del Diritto, che studia l'applicazione

dell'informatica nel Diritto. Questa connessione ci porta all'idea di un Diritto di tipo orizzontale o trasversale (sebbene specializzato), che estende i suoi effetti sulla maggior parte dei rami e delle versanti giuridiche come emanazione di quello strumento da cui nasce come conseguenza del suo effetto diffusivo e a cui si accompagnerà in maniera intrinseca: Internet.

**III.** All'interno del contesto descritto, nell'UE e in Spagna nascono la DCE e la LSSICE, rispettivamente. Entrambe le norme introdurranno e generalizzeranno un concetto finora sconosciuto, ma di grande importanza, dato che da esso deriverà tutta la rete che articola normativamente, in maniera diretta o indiretta, la società digitale. Ci riferiamo ai SSI, che si caratterizzano per essere forniti: *a distanza*, cioè senza la presenza fisica della persona che fornisce il SSI (PSSI, concetto di recente creazione) e il suo destinatario (DSSI, denominazione anch'essa innovativa); *per via elettronica*, poiché è inviato dalla fonte e ricevuto dal DSSI tramite apparecchiature elettroniche di elaborazione (compresa la compressione digitale) e di memorizzazione di dati e trasmesso, canalizzato e ricevuto integralmente via cavo, radio, procedimenti ottici e ogni altro supporto elettromagnetico; su richiesta individuale di un destinatario di servizi, poiché è quest'ultimo a richiedere che il servizio gli sia offerto, e, di solito, in modo oneroso, poiché tanto il PSSI quanto il DSSI forniscono una prestazione reciproca a favore dell'altra parte.

**IV.** A essi dobbiamo aggiungere i SSIi, SSI strumentali o accessori il cui scopo è proprio quello di fornire la prestazione (al PSSI) o l'utilizzo (al DSSI) di SSI, o permettere (al PSSI o al DSSI) l'accesso a una determinata informazione.

Inizialmente, e per inclusione diretta perché riconosciuti come tali, si comprendono all'interno di questo gruppo: in primo luogo, i servizi riguardanti l'accesso a Internet (*Internet service providers*), i cui fornitori sono vincolati al regime di responsabilità previsto dagli articoli 12 DCE e 14 LSSICE; in secondo luogo, quelli che rendono possibile la trasmissione di dati da reti di telecomunicazione (*mere conduit* o *routing*), con i loro fornitori sottomessi a quanto stabilito dai precetti precedenti; in terzo luogo, i servizi riguardanti la realizzazione di copie temporanee dei siti Internet richiesti dagli utenti o dai destinatari (*proxy caching* o *memoria tampón*), la cui eventuale responsabilità si contiene negli articoli 13 DCE e 15 LSSICE; in quarto luogo, vi sonoi servizi che, nei server stessi, permettono l'*hosting* di dati, applicazioni o servizi forniti da altri, dove i soggetti incaricati della loro fornitura verranno sottomessi a quanto stabilito dagli articoli 14 DCE e 16 LSSICE, e, in ultimo,

quelli che forniscono strumenti di ricerca, accesso e memorizzazione di dati e link ad altri siti Internet (*searching and linking*), previsti legalmente per la prima volta nell'articolo 17 LSSICE, e che non possiedono un equivalente nella DCE.

**V.** Un SSI per eccellenza è il commercio elettronico considerato, in termini generali, come quell'insieme di dati che, trasmessi tramite i meccanismi che forniscono le nuove tecnologie dell'informazione e della comunicazione, perseguono fini di tipo negoziale, cioè, di compravendita di beni o prestazione di servizi, ivi comprese le trattative preliminari e ulteriori attività dello stesso genere, anche se non sono strettamente contrattuali.

Questa trasformazione della relazione commerciale in rapporto digitale renderà possibile, tra l'altro, un aggiornamento e una miglioria del sistema, della parità di opportunità, della possibilità di acquisire beni e servizi senza restrizioni orarie o geografiche di nessun tipo, dell'apparizione di nuove opportunità di affari o dell'allargamento delle possibilità effettive di scelta. In ogni caso, non sarà esente da rischi e svantaggi con una conseguente esigenza di controllo. Tali rischi derivano, in sostanza, dalla problematica di ricevere prodotti sbagliati o difettosi per acquisti, per così dire, *alla cieca* (che, a modo di circolo vizioso, accentuerebbero la diffidenza verso il mercato virtuale), oppure dall'incremento della leggerezza dei DSSI nel processo di acquisto.

Per il resto, il commercio elettronico si compone di due attività fondamentali che raggruppano le restanti: da un lato, l'invio di comunicazioni commerciali precedenti alla contrattazione riguardanti la diffusione di informazioni di questo tipo per via telematica, e, dall'altro, la contrattazione telematica vera e propria, in cui rientra l'organizzazione o la gestione delle aste in forma telematica, o di mercati e centri commerciali virtuali e la gestione di acquisti per via elettronica da gruppi di persone.

**VI.** Le comunicazioni commerciali per via telematica dovranno soddisfare le prescrizioni degli articoli 6-8 DCE e 19-22 LSSICE per essere valide ai fini giuridici. Tali prescrizioni sono le seguenti: in primo luogo, devono essere chiaramente identificabili, non potendosi nascondere sotto falso nome tale da indurre in errore chi le riceve; in secondo luogo, devono identificare con esattezza la persona, fisica o giuridica, per conto della quale si inviano le cosiddette comunicazioni, e, in terzo luogo, devono descrivere minuziosamente le offerte promozionali e i concorsi o i giochi promozionali che, eventualmente, le accompagnano, a patto che siano consentiti nello Stato membro in cui sia stabilito il PSSI, siano accessibili

facilmente e si presentino in maniera chiara e inequivocabile le condizioni da rispettare per ottenerli.

Meno univoca sarà, invece, la questione rispetto a come trattare da un punto di vista legale lo *spamming* o l'invio massiccio e indiscriminato di comunicazioni virtuali di tipo pubblicitario o promozionale tramite posta elettronica, oppure un altro mezzo equivalente, che non siano state richieste previamente o espressamente autorizzate dai destinatari delle stesse. Al riguardo, due sono state, tradizionalmente, le opzioni di politica legislativa che determinano la liceità o illiceità della posta elettronica indesiderata: una prima opzione raggruppa i cosiddetti sistemi *opt-out*, che permettono di inviare pubblicità indesiderata a tutti i destinatari che non abbiano optato per non riceverla, dovendo dare al destinatario la possibilità di esigere che non gli sia inviata dell'altra pubblicità; una seconda opzione, che raggruppa i cosiddetti sistemi *opt-in*, è quella per cui il messaggio pubblicitario è lecito soltanto se il destinatario ha scelto in precedenza di ricevere comunicazioni commerciali, per cui non basta non opporsi (sistema *opt-out*), ma deve esserci una esplicita richiesta, oppure un rifiuto chiaro di invio.

A livello comunitario, l'articolo 7 DCE opta per la prima modalità imponendo, oltre ad altri requisiti stabiliti dal Diritto comunitario, che gli Stati membri che consentono le comunicazioni commerciali inviate da PSSI stabiliti nel territorio ma non richieste dai DSSI, garantiscano che queste siano identificabili in maniera chiara e inequivocabile nel momento stesso della loro ricezione senza comportare costi aggiuntivi per il destinatario. Inoltre, si esige l'adozione di tutte quelle misure necessarie a garantire che i PSSI che realizzano queste comunicazioni commerciali non richieste prima consultino regolarmente e poi rispettino gli elenchi di esclusione volontaria in cui si potranno iscrivere le persone fisiche che non desiderano ricevere tale pubblicità. A questo proposito, ci chiediamo perché soltanto le persone fisiche possono accedere a questi elenchi, e concludiamo che, con ogni probabilità, il motivo è legato alla protezione supplementare che meritano quegli individui che, da una condizione di consumatore, utilizzano un SSI nell'ambito di una attività non professionale. Ciononostante, con questa previsione normativa si stabilisce una nota discriminazione tra quelle persone giuridiche che agiscono nell'ambito della loro attività professionale e che hanno difficoltà ad iscriversi negli elenchi di esclusione volontaria di comunicazioni commerciali non richieste, e le persone fisiche che, come le

precedenti, si muovono all'interno della loro professione o dei loro affari quando utilizzano un SSI e che, non trovandosi nemmeno loro in quella situazione svantaggiata e necessaria di protezione, possiedono questo diritto.

Invece, l'articolo 21 LSSICE opta per un approccio radicalmente opposto. Infatti, diversamente dalla politica legislativa difesa dalla norma europea, la Legge spagnola propende per un sistema *opt-in*, determinando la liceità della comunicazione commerciale soltanto se, previamente, il DSSI o destinatario ha richiesto l'invio o ha dato espressamente il suo consenso, senza che sia sufficiente una sua mera non opposizione. Costituisce un'eccezione a questa regola generale quella indicata nel secondo paragrafo di questa disposizione, per cui l'invio di pubblicità mediante la Rete sarà legale quando ci sia una relazione contrattuale previa tra l'emittente (PSSI) e il destinatario (DSSI) del messaggio, a patto che il primo abbia ottenuto i recapiti del DSSI in modo lecito e li utilizzi soltanto per l'invio di comunicazioni commerciali riguardanti prodotti o servizi della propria azienda che siano simili a quelli che, in precedenza, furono oggetto di contrattazione dal cliente. Comunque, il PSSI avrà l'obbligo di offrire al DSSI la possibilità di opporsi al trattamento dei suoi dati per finalità promozionali tramite una procedura semplice e gratuita sia al momento della raccolta dei dati sia in ognuna delle comunicazioni commerciali inviate.

**VII.** Già nell'ambito della contrattazione elettronica vera e propria occorrerà esprimere, attraverso un'analisi previa e innovativa, vista la sua rarità, la controversa natura giuridica del documento come elemento originale da cui quella si sviluppa. A questo proposito, conviene sottolineare l'esistenza di due teorie tradizionali e antagoniste che saranno superate grazie a un'ipotesi personale e più aggiornata della nuova realtà digitale.

La prima di queste teorie è nota come *teoria rigida, dello scritto, ristretta o latina*, che sostiene che il documento deve essere sempre formulato per iscritto su supporto fisico e il supporto fisico su carta, identificando, erroneamente a mio parere, questi termini come sinonimi. Questa visione primitiva del documento si fonda sull'assoluta ignoranza, in passato, in merito ai progressi tecnologici che poi si sono verificati in maniera indiscutibile nella nostra società, facendo sí che diversi corpi legali passati si ritrovino a far uso di questa erronea equivalenza di termini. Questo è quanto succede con il Codice Civile e l'ALECiv che usano sempre la parola *scritto* al posto dell'espressione, più corretta, di *supporto fisico cartaceo*, senza considerare che tutti i documenti avranno un contenuto scritto e che non

solo i documenti in supporto fisico cartaceo ricorreranno alla scrittura come mezzo di rappresentazione della parola oppure dell'idea.

La seconda teoria, che prende il nome di *teoria della rappresentazione o germanica*, si manifesta dal momento in cui emergono fortemente i progressi consentiti dal mondo digitale che obbligano a riconsiderare l'idea di documento da intendersi, invece, come un concetto certamente di più ampia gittata. Questa corrente trova la sua origine nella distinzione fatta da CARNELUTTI tra *fonti di prova* e *mezzi di prova*. Il problema che comporta questa idea è la sua eccessiva vastità, dato che, nuovamente, identifica *documento* con *supporto fisico cartaceo* e *supporto fisico cartaceo* con *scritto*, oltre a confondere il supporto del documento con la natura (elettronica) dell'informazione che riflette. Inoltre, non considera il fatto che il nuovo documento elettronico può anche comparire come supporto fisico e cartaceo (o, addirittura, audiovisuale) e con un materiale che non è più necessariamente la carta, ma uno distinto, anche se pur sempre adatto per la registrazione di questo tipo di contenuto. Questa confusione costituirà proprio la base dottrinale per far sì che la LECiv attuale riconosca legalmente i documenti elettronici come mezzo di prova (articoli 299.2 e 382 a 384), ma con il nome di *strumenti*, e li consideri fuori dalla prova documentale (articoli 299.1.2.º e 3.º e 317 a 334).

Da qui si sviluppa una teoria, personale e finora sconosciuta, che consente di mettere in luce il fatto che l'unico cambiamento apportato dall'introduzione delle nuove tecnologie dell'informazione e della comunicazione è l'ampliamento, come conseguenza dell'apparizione dell'elettronica, della varietà dei materiali e dei supporti fisici, adesso in grado di ospitare non solo dati affidabili e suscettibili di utilizzo per provare qualcosa non solo in forma scritta (attuale definizione di *documento* contenuta nella RAE), ma pure in forma visuale oppure orale. Questa nuova teoria, che potremmo chiamare *teoria del documento come contenuto*, allarga la nozione di documento partendo dalla parola scritta e estendendola all'immagine e al suono che, ormai, (fondamentalmente grazie alla promulgazione del RIE-SCTE) si possono archiviare per il loro posteriore utilizzo come mezzo di prova in un processo giudiziario. Ciò è sintetizzato in una proposta di definizione di documento esposta di seguito: *contenuto conservato in un supporto fisico cartaceo oppure un altro materiale adeguato che dà informazione, scritta, visuale o orale, affidabile o rilevante relativa a fatti con efficacia probatoria oppure per qualsiasi altro tipo di utilità giuridica*. Ciò che davvero importa, quindi, non è il materiale (carta o qualsiasi altro adatto per l'archiviazione dell'informazione) di cui è fatto il supporto fisico in cui compare il documento, ma la sua idoneità per l'uso come

mezzo di prova nel processo e il fatto che si accompagni, a sua volta, a tanti altri strumenti, quali la firma elettronica, che offrono una ulteriore sicurezza per quanto riguarda l'esistenza della relazione giuridica, l'identificazione del/degli autore/i del documento e la stessa integrità dell'informazione che in esso si plasma.

Conviene anche sottolineare a tal proposito l'articolo 9.1 DCE e, ancora di più, l'articolo 23.1 e 3 LSSICE, che cercano di risolvere il problema, ereditato nel tempo, dell'identificazione erronea tra *documento* e *supporto*, tra *supporto fisico cartaceo* e tra *supporto fisico cartaceo* e *scritto*. E lo fanno ricorrendo al noto *principio di equivalenza funzionale* proprio del Diritto della contrattazione elettronica che si fonda sulla possibilità di rispettare i requisiti legali di forma tramite l'utilizzo di formule elettroniche adeguate agli obiettivi e alle funzioni a cui tradizionalmente corrispondono. Grazie a questo principio, la funzione giuridica che svolgerebbe, in tutta la sua estensione, la strumentazione autografa del documento tradizionale elaborato su un supporto fisico cartaceo (eventualmente anche nella sua forma orale) riguardante qualsiasi tipo di atto giuridico, si potrebbe soddisfare anche con la strumentazione digitale (scritta, visuale e sonora) del documento contenuto su un supporto fisico diverso dal cartaceo, ma adeguato per l'archiviazione dell'informazione di natura elettronica, al di là della portata e delle finalità dell'atto così configurato. In questo modo, in pratica, riusciamo a far rispettare gli effetti giuridici perseguiti dal mittente della dichiarazione di volontà indipendentemente dal supporto su cui viene riportata questa dichiarazione. Tuttavia, sebbene raggiunga l'obiettivo per cui fu creato, il principio di equivalenza funzionale contenuto nell'articolo 23.3 LSSICE utilizza termini, dal mio punto di vista, migliorabili: nello specifico, con la redazione attuale della norma si mantiene l'errore di concetto e di identificazione più volte criticato, e semplicemente si "mette una pezza" per evitare i suoi effetti deleteri e rendere operativa l'introduzione del mondo digitale nell'ambito del Diritto tramite la formula, adeguata ma concepita in termini sbagliati, dell'equivalenza funzionale. Una redazione della legge con fini più ambiziosi potrebbe essere stata redatta nel seguente modo: *a patto che la Legge esiga che il contratto o qualsiasi informazione a riguardo si riporti per iscritto, questo requisito sarà ritenuto soddisfatto se il contratto o l'informazione si riporti pertanto su supporto fisico cartaceo o su supporto fisico diverso dal cartaceo ma idoneo per l'archiviazione di informazione di natura elettronica*. In questo modo, verrebbero rispettate in una maniera più soddisfacente le esigenze contenute nella normativa per le tradizionali funzioni del mal concepito *scritto*, cioè, del documento su supporto fisico cartaceo.

Comunque, da una prospettiva puramente negoziale, quanto precedentemente detto determinerà la base per giustificare l'apparizione del contratto elettronico, in modo tale che quei contratti perfezionati attraverso l'uso delle nuove tecnologie non potranno avere peggiore (né migliore) considerazione giuridica di quelli che vengano redatti con mezzi convenzionali e tradizionali. Arriviamo, quindi, a quello che è ritenuto come il *principio di non discriminazione*, che sarebbe, rispetto all'equivalenza funzionale, la faccia, espressa in termini negativi, della stessa medaglia.

**VIII.** Entrando nel merito di quei contratti in cui sia l'offerta che l'accettazione si trasmettono tramite apparecchiature elettroniche di elaborazione e di memorizzazione di dati collegate a una rete di telecomunicazioni, conviene sottolineare il rinnovato ruolo assunto dal *principio generale spiritualista, di libertà delle forme o consensualista,* tradizionale nel nostro Diritto. Questo principio afferma che quel che davvero importa per poter parlare di un contratto elettronico valido ed efficace non è la forma, ma l'aspetto consensuale o spirituale; in tal senso, da quando c'è il consenso esiste il contratto a prescindere dalla registrazione e del supporto fisico utilizzati dalle parti per manifestarlo.

Il motivo di questo nuovo ruolo va ricercato nella inclusione del mondo virtuale, per il quale si impone l'obbligatorietà del supporto: mentre il contratto tradizionale poteva essere stipulato in modo valido in forma scritta oppure orale (la prima senza bisogno di forma speciale, e la seconda bisognosa di supporto fisico), il contratto elettronico, a prescindere dalla forma, si dovrà realizzare obbligatoriamente in modo digitale. Per questo motivo, anche se non è necessaria *a priori* la sua attestazione in supporto fisico diverso dal cartaceo ma che sia adeguato per l'archiviazione di informazione di natura elettronica, come presupposto per la validità del contratto dalla concezione tradizionale di questa esigenza, è chiaro che l'inosservanza di questo requisito determinerà la stessa inesistenza del contratto per mancanza di qualsiasi forma, di quelle elettronicamente possibili, di codici criptati o di linguaggi speciali. Possiamo parlare allora di una formalità, se si vuole, più profonda o strutturale, piuttosto che pretesa o legale, precettiva, per la validità dell'atto da un punto di vista non tanto giuridico quanto naturale o sostanziale. Di conseguenza, il contratto elettronico risponde, allo stesso tempo e in modo inseparabile, alla duplice finalità della forma *ad substantiam* e *ad probationem*: la prima, per la necessità del supporto come concretizzazione necessaria dell'immaterialità intrinseca del negozio giuridico; la seconda, come mezzo indispensabile per la prova, non più della sua validità, ma della sua

vita o esistenza. Parliamo, così, di quello che potremmo chiamare *formalismo indiretto* o *formalismo necessario di contratti giuridicamente non formali*, cioè i contratti elettronici.

In ogni caso, lo stesso consenso, che, com'è stato detto, è necessario per ritenere perfezionato il contratto, costituirà anch'esso una questione polemica nell'ambito del Diritto contrattuale elettronico per la controversia circa la delimitazione temporale del momento in cui debba ritenersi realizzato l'accordo fra le parti. Un primo punto di vista viene proposto dalla *teoria della cognizione*, contenuta nella redazione previa dell'articolo 1262.2, *ab initio*, Codice Civile, che sostiene che l'accettazione dell'offerta produrrà soltanto gli effetti che risultano propri dal momento in cui l'offerente l'abbia conosciuta. Il problema di questo approccio è che la stipulazione del contratto si subordinava all'effettivo recupero del messaggio dati dal PSSI, facendo sí che la condotta poco diligente di chi realizza l'offerta possa ostacolare la stipula e possa, di conseguenza, danneggiare un DSSI che in ogni momento ha agito in buona fede inviando la sua accettazione o conformità. Un secondo punto di vista è quello conosciuto come *teoria della ricezione*, che, invece, afferma che non occorre che l'offerente abbia conosciuto, in maniera effettiva, l'accettazione della controparte, ma è sufficiente che l'abbia semplicemente potuta conoscere, cioè, che questa sia arrivata al suo ambito di controllo. In terzo luogo, troviamo *la teoria della spedizione o emissione*, assunta inizialmente dall'articolo 54 CCom, secondo la quale non basta che l'accettante abbia manifestato la sua accettazione, ma occorre averla inviata all'altra parte, cioè occorre che l'accettazione sia uscita dall'ambito di controllo. Infine, e come estremo opposto alla teoria della cognizione, troviamo la *teoria della dichiarazione o manifestazione*, che esige, soltanto, che il destinatario dell'offerta abbia manifestato la volontà di accettarla, senza nemmeno la necessità di averla inviata. Ebbene, dopo la promulgazione della D. A. 4ª LSSICE si è verificata la fusione dei due sistemi, quello civile (articolo 1262 CC) e quello commerciale (articolo 54 CCom), ed è scomparsa la disparità di criteri che c'era fino a quel momento tra entrambe le disposizioni; viene, quindi, stabilito un criterio comune riguardante i contratti a distanza in primo luogo, e i contratti elettronici in generale successivamente, e un criterio speciale per i contratti elettronici stipulati tramite dispositivi automatici.

Il primo di questi criteri, applicabile ai contratti a distanza in generale, determina che «trovandosi in posti diversi chi ha proposto l'offerta e chi l'ha accettata, c'è consenso dal momento in cui l'offerente conosce l'accettazione o, avendola trasmessa all'accettante, non può ignorarla senza mancare di buona fede». In questo modo, accoglie la *teoria della*

*ricezione*, aggiungendo che, nel caso in cui si conosca l'accettazione (*teoria della cognizione*), a maggior ragione si riterrà perfezionato il contratto.

Il secondo riguarda i contratti elettronici stipulati attraverso lo scambio di messaggi di posta elettronica o simili, previsto nell'articolo 28.2 LSSICE, e offre un criterio per determinare il momento della ricezione: cioè, quando la parte a cui si indirizza l'accettazione può essergli nota. Tuttavia, la norma non contiene nessun criterio che permetta di sapere cosa dobbiamo considerare quando parliamo di *attestare* l'accettazione. A tal fine forse è possibile applicare per analogia il criterio che invece presenta la LSSICE nel secondo paragrafo di quel precetto riguardante l'attestazione di ricevuta dell'accettazione tramite un avviso di ricezione; di conseguenza, e in linea con quanto previsto dalla *teoria della ricezione*, basterebbe che l'accettazione del DSSI fosse arrivato al posto giusto affinché il PSSI potesse accedere al suo contenuto, evitando che la perfezione del contratto venga lasciata alla discrezione di chi, potendo conoscere l'accettazione dell'offerta negoziale, invece non lo facesse per negligenza o mancanza di diligenza necessaria.

Nell'ambito di questi contratti elettronici, verrà stabilito, finalmente, un criterio speciale riguardante soltanto quei contratti stipulati tramite dispositivi automatici in cui riteremo che c'è consenso dal momento in cui viene manifestata l'accettazione, come secondo la *teoria della spedizione*.

**IX.** Un passo successivo nella nostra ricerca sarà determinato dalla necessità di analizzare, nell'ambito dei contratti elettronici, quelli provvisti di firma, la quale, in virtù del sopracitato principio di libertà delle forme, non sarà, in generale, un elemento essenziale e determinante per la validità ed efficacia degli stessi, ma bensì un complemento fondamentale ai fini di prova del loro contenuto, autorità e integrità. A tal proposito, conviene sottolineare l'importanza della recente entrata in vigore del RIE-SCTE che, oltre ad abrogare la DFE ed essere direttamente applicabile in ognuno degli Stati membri, promuoverà una situazione d'incertezza manifesta a livello interno, motivata dall'esistenza di una norma che non risponde più, in tutta la sua integrità, ai cambiamenti motivati dal nuovo Regolamento. Questo è il motivo per il quale si trattano in parallelo gli effetti che implicherebbe l'applicazione del non ancora ratificato ALSEC, analizzando le somiglianze e differenze che presenta nei confronti dell'attuale LFE. In ogni caso, il nuovo contesto tratterà, com'è normale, la regolamentazione che esiste su questa materia negli ordinamenti giuridici spagnolo e italiano, riflettendone l'evoluzione normativa di entrambi.

**X.** Ne consegue, a questo punto, lo sviluppo di un concetto trascendentale, forse uno dei più importanti per spiegare il funzionamento della nuova normativa comunitaria e, di conseguenza, della firma elettronica come strumento essenziale per generare sufficiente fiducia nell'uso del commercio elettronico: parliamo dei SSIisc, sottospecie che integra per via indiretta e come frutto della ricerca realizzata i SSIi. Se analizziamo la natura dei SSIisc contenuti nel Regolamento eIDAS possiamo osservare che, allo scopo di facilitare la prestazione o l'utilizzazione di altri SSI (funzione di intermediazione propria di qualsiasi SSIi), questi di solito saranno anche prestati in cambio di una remunerazione a distanza, tramite la via elettronica e sotto richiesta individuale del DSSIisc.

In questo modo, insieme ai SSIi previsti negli articoli 12-14 DCE e 14-17 LSSICE (riguardanti la fornitura di servizi di accesso a Internet, la trasmissione di dati per reti di telecomunicazioni, l'hosting negli stessi server di dati, applicazioni o servizi forniti da altri e la fornitura di strumenti di ricerca, accesso e raccolta di dati o links su altri siti di Internet), i SSIisc previsti negli articoli 3.16) e 17) e 13-45 RIE-SCTE chiudono o, almeno, delimitano di più il cerchio di SSIi di applicazione all'interno dell'ordinamento giuridico spagnolo. Tra questi servizi si includeranno, nello specifico, quelli che rendono possibile sia la creazione, la verifica e la validazione di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, servizi elettronici di recapito certificato, certificati riguardanti questi servizi e certificati di autenticazione di siti web, sia la conservazione di firme, sigilli o certificati elettronici riguardanti questi servizi (*trust services*) o qualsiasi altro servizio prestato sotto richiesta individuale degli utenti, purché rappresentino un'attività economica per il PSSIi.

In questo caso specifico potremmo concludere che il SSI sarebbe rappresentato dalla contrattazione elettronica di beni e servizi, mentre i concreti SSIi che facilitano la loro prestazione, oltre a tutti quelli che possano esserci in virtù degli articoli 12-14 DCE e 14-17 LSSICE, sarebbero quelli riguardanti la creazione, la verifica, la validazione e la conservazione di firme elettroniche, così come i loro corrispondenti certificati che avranno la natura di SSIisc.

**XI.** Stando così le cose, la firma elettronica si considera come la manifestazione per eccellenza dell'importante principio di equivalenza funzionale proprio del Diritto della contrattazione elettronica e come la soluzione tecnica più adeguata per provare l'esistenza dell'au-

torità, integrità o non riconoscibilità di questi contatti. Di conseguenza, abbiamo realizzato un'analisi di ognuno degli elementi che costituiscono la firma elettronica nelle sue diverse modalità per offrire un approccio più adeguato alla stessa.

Tra questi elementi possiamo sottolineare, in primo luogo, la crittografia, strumento essenziale che permette di dotare di sicurezza la trasmissione e l'archiviazione dei dati riguardanti i contratti elettronici che circolano attraverso le reti informatiche. Così, grazie alla trasformazione del messaggio, soltanto le persone in possesso degli algoritmi (processo matematico) e delle chiavi (insieme di cifre alfanumeriche) adeguati potranno accedere al suo contenuto in maniera corretta e soddisfacente.

Quando è bilaterale ed elettronica, l'informazione contenuta in un messaggio di dati è criptata dal mittente con lo scopo di rendere il suo contenuto accessibile soltanto dal destinatario legittimo, e a tal fine esiste una serie di chiavi che potranno intervenire in due diversi scenari: un primo scenario secondo il quale la stessa chiave è conosciuta da tutte e due le parti (*crittografia simmetrica, a chiave condivisa, a chiave privata o di una chiave*), e un secondo scenario in cui ogni chiave è conosciuta soltanto dalla parte che la possiede (*crittografia asimmetrica o a chiave pubblica)*. Con questo ultimo metodo, certamente più sicuro del precedente, facciamo in modo che il messaggio di dati non sia sottoposto a cambiamenti nel corso del processo di invio e ricezione (integrità) e che soltanto il destinatario legittimo (unico in possesso della chiave privata corrispondente a quella concreta chiave pubblica, che si autentica nell'eseguire il processo di coincidenza di chiavi e garantisce così l'identificazione autenticata del destinatario e la non riconoscibilità nella destinazione) possa leggere il contenuto di questo messaggio senza poter essere decifrato, nemmeno dalla persona che l'ha inviato (confidenzialità).

Tuttavia, con questo metodo non c'è modo di sapere se il mittente del messaggio di dati è chi dice di essere (identificazione autenticata del mittente). La firma digitale risolve questo problema partendo dal metodo di crittografia a chiave pubblica, ma in maniera inversa. Ora è il mittente che cripta il documento elettronico con la sua propria chiave privata, e può essere decifrato soltanto da chi è in possesso della corrispondente chiave pubblica, anch'essa di proprietà del mittente e che matematicamente è correlata alla prima e a cui può accedere chiunque.

Sebbene siano esposti in maniera separata, entrambi i metodi crittografici asimmetrici potrebbero realizzarsi insieme tramite due cifrature sequenziali. Infatti, in un primo passo

il mittente cripterebbe il messaggio di dati con la sua chiave privata rendendo possibile la firma elettronica che garantirebbe l'identificazione autenticata del firmatario e l'integrità e la non riconoscibilità dell'origine del contenuto del documento una volta decifrato con la chiave pubblica del firmatario. In un secondo momento, il firmatario cripterebbe il messaggio di dati con la chiave pubblica del destinatario; un messaggio di dati che, una volta decifrato dal destinatario con la sua corrispondente chiave privata, permetterebbe la non riconoscibilità alla consegna e la confidenzialità del documento.

Nella firma elettronica, quindi, queste chiavi private corrispondono quelli che sono definiti *dati di creazione di firma elettronica*, cioè gli unici dati che utilizza il firmatario per creare una firma elettronica. Questi dati saranno accompagnati inseparabilmente da un dispositivo di creazione, cioè dalle apparecchiature informatiche o software configurati utilizzati per creare una firma elettronica che potrà essere autorizzato se rispetta i requisiti normativamente imposti per dare un livello di sicurezza superiore. A loro volta, e come elementi che chiudono il funzionamento della firma elettronica, troviamo i dati di verifica (nell'ambito del sistema di firma digitale, le chiavi pubbliche) che vengono utilizzati per convalidare una firma elettronica tramite la loro applicazione nei relativi dispositivi di verifica o convalida.

Un secondo elemento, indispensabile in quelle firme elettroniche dotate di un livello di sicurezza più alto, sarà il certificato di firma elettronica, un documento elettronico di natura privata emesso da un PSSIisc attraverso il quale, nel contesto della cosiddetta *infrastruttura a chiave pubblica* (PKI), certifica e sostiene, con l'applicazione della sua propria chiave privata, l'identità digitale di persone e l'autenticità delle comunicazioni e dei documenti che queste potrebbero creare. In tal senso, dopo una verifica preliminare dell'identità del richiedente della certificazione (firmatario), si attesta che questo è effettivamente il proprietario di una determinata chiave pubblica e non un terzo soppiantatore. Nel caso in cui siano ritenuti idonei, questi certificati apporteranno un maggior valore e una maggiore sicurezza poiché sono stati emessi rispettando determinate esigenze riguardanti il loro contenuto, le procedure di verifica dell'identità del firmatario e l'affidabilità e le garanzie dell'attività di certificazione elettronica.

**XII.** Questo ci mette davanti alla firma elettronica vera e propria, più concretamente davanti alle firme elettroniche corrispondenti ad ognuna delle tre classi previste dalla normativa

nazionale e comunitaria e alla sua evoluzione a seguito dell'entrata in vigore del Regolamento eIDAS.

La prima è la *firma elettronica generale*, che è quella firma elettronica integrata da qualsiasi metodo o simbolo basato su mezzi elettronici che si utilizza o adotta da una parte con lo scopo di firmare, rispettando tutte o alcune funzioni caratteristiche della firma autografa. Questa definizione, esposta dalla nuova normativa europea, incorre, come possiamo osservare, in una sorta di ridondanza piuttosto incomprensibile che induce a definire la firma elettronica generale come quella che utilizza il firmatario per firmare. A questo proposito, il RIE-SCTE si allontana dalla definizione del suo predecessore, la DFE, che, offrendo un concetto di firma elettronica semplice (non generale), limitava l'obiettivo comune perseguito da qualsiasi firma elettronica per servire come mezzo *di autenticazione*; e tutto questo con una redazione, a mio parere, discutibile e che genera confusione, in quanto, trattandosi questa di una fase di autenticazione posteriore rispetto a quella di identificazione vera e propria, sarebbe stato meglio optare per quest'ultima, come giustamente fa, precisamente, il legislatore spagnolo sia nell'originario articolo 2.a) RDLFE sia nell'articolo 3.1 LFE, entrambi dedicati alla firma semplice come mezzo che permette, in ogni caso, di *identificare la persona che firma* in relazione a certi dati, a prescindere dal fatto che, posteriormente, si constati che la persona fisica che firma il documento elettronico è chi dice di essere. Tuttavia, è certo che nessuna chiarisce cosa dobbiamo intendere per autenticazione e identificazione, e questo ci mette davanti a un concetto giuridico indeterminato soggetto a interpretazioni radicalmente diverse.

In ogni caso, la verità è che, con la nuova redazione, il Regolamento comunitario non permette al giurista la concretizzazione dell'elemento che, una volta soddisfatto, permetta di far capire quando ci troviamo davanti a una firma elettronica pur essendo basica o elementale. Di conseguenza, all'interno di questa definizione, rientrerebbero procedure multipli di firma, alcune di esse così complessi come la firma digitale basata sulla crittografia asimmetrica o la firma configurata sulla base di sistemi biometrici come ad esempio l'iride, il palmo della mano o l'impronta digitale, e altri piuttosto semplici come l'inclusione del nome oppure un altro elemento identificativo alla fine di un messaggio di posta elettronica, la firma autografa digitalizzata o l'esistenza di una domanda-risposta e di un PIN di accesso. Pertanto, possiamo affermare che, se lo scopo perseguito è generare certezza nelle persone soggette e colpite diretta o indirettamente dalla norma, sarebbe meglio riformulare il concetto attuale di firma elettronica generale e riorientarlo, con sfumature, a

quello tradizionale di firma elettronica semplice in una sorta di definizione almeno un po' più chiara o completa, che potrebbe essere quella indicata di seguito: *la firma elettronica è l'insieme di dati in formato elettronico, allegati ad altri dati elettronici o associati in modo logico tra di loro, utilizzati, perlomeno, come mezzo di identificazione del firmatario.*

Aumentando i requisiti di qualità e di sicurezza della firma elettronica, l'articolo 3.11) RIE-SCTE mantiene il concetto di *firma elettronica avanzata* esistente in precedenza, considerandola: quella firma elettronica vincolata al firmatario in modo unico, che permette l'identificazione elettronica del firmatario, che è stata creata utilizzando dati di creazione di firma elettronica che il firmatario può utilizzare per la creazione di una firma elettronica con un alto livello di fiducia sotto il suo proprio controllo esclusivo ed, infine, che è vincolata ai dati firmati da se stessa in modo tale che qualsiasi modifica ulteriore di questi dati sia rilevabile. Si noti che con i primi tre requisiti (vincolo unico con il firmatario, identificazione di quest'ultimo e creazione attraverso mezzi posti sotto il suo controllo) si cerca di garantire l'identificazione autenticata dell'autore e di evitare il rifiuto in origine del messaggio di dati); invece, con l'ultimo (vincolo con i dati, permettendo di scoprire qualsiasi modifica ulteriore) si cerca di proteggere l'integrità del documento elettronico.

Infine, nel livello più alto troviamo la *firma elettronica qualificata*, prima chiamata *firma elettronica riconosciuta*, definita come la firma elettronica avanzata che rispetta due requisiti fondamentali: essere creata tramite un dispositivo qualificato di creazione e fondarsi su un certificato qualificato di firma elettronica. Come possiamo osservare, più che una nuova modalità, la firma elettronica qualificata è un nuovo tipo di firma elettronica avanzata accompagnata da determinati elementi che le danno una affidabilità maggiore. Per questo motivo riceve un nuovo *nomen iuris* con la finalità di distinguerla da quelle altre che, per non essere state generate tramite un dispositivo qualificato di creazione o per il non basarsi su un certificato qualificato di firma elettronica (o per non rispettare nessuno di questi due requisiti), non avranno effetti legali paragonabili, in termini di validità ed efficacia, a quelli che ha la firma elettronica qualificata, integrandosi nella firma elettronica avanzata. Quest'ultima, proprio come la firma elettronica semplice e la firma elettronica avanzata basata su un certificato elettronico qualificato, non sarà esente né da effetti giuridici né di ammissibilità come prova in processi giudiziari per il semplice fatto di possedere una forma elettronica o per non rispettare i requisiti della firma elettronica qualificata, con l'obbligo di valutare, in ogni caso, la loro efficacia, un aspetto cosa che a volte può essere complesso e oneroso.

Per il resto, e in virtù del principio di autonomia della volontà, le parti saranno libere di fissare le condizioni per l'uso della firma elettronica *inter partes* oltre a quanto previsto dalla norma, che non sarà di applicazione in questi casi tranne in modo supplementare, disciplinando principalmente i termini stabiliti nel contenuto dell'accordo: questo è ciò che chiamiamo *firma elettronica convenzionale*, accolta in modo implicito dall'articolo 2.2 RIE-SCTE. Ciononostante, non mancano autori che hanno manifestato il pericolo di questa misura, particolarmente in quei casi in cui dalla fissazione dei termini di funzionamento della firma elettronica dalle parti deriva una situazione di disuguaglianza tra di loro; tuttavia, in caso di non incorrere in problemi simili, è certo che, adattandole alle necessità delle parti (che possono richiedere aspetti non previsti o diversi da quelli previsti legalmente), possono risultare positive per ottenere una risposta più soddisfacente alle loro necessità particolari.

**XIII.** Grazie a questa maggiore esigenza di sicurezza, la firma elettronica qualificata avrà nei confronti dei dati contenuti in forma elettronica lo stesso valore della firma autografa nei confronti dei dati consegnati su supporto cartaceo. Si manifesta di nuovo e fortemente il principio di equivalenza funzionale che cerca di attribuire, per quanto possibile, le stesse conseguenze giuridiche all'ambiente fisico e all'ambiente virtuale.

Fin qua, tutto uguale. Tuttavia, il nuovo Regolamento aggiunge una novità riguardo al corpo normativo precedente, visto che aggiunge esplicitamente una proprietà addizionale alle firme elettroniche create da dispositivi qualificati e fondati su certificati qualificati. Questa proprietà consiste nell'equiparazione comunitaria di firme elettroniche qualificate, firme che, sorte in uno Stato membro qualsiasi, dovranno essere riconosciute anche in tutti gli altri.

Nel caso di firme elettroniche non qualificate, come anticipavamo, non saranno prive di effetti giuridici per il semplice fatto di essere firme elettroniche o perché non rispettano i requisiti della firma elettronica qualificata. In questo modo, mentre la firma elettronica qualificata gode di effetti legalmente determinati, qualsiasi firma elettronica che non sia qualificata potrà godere, o meno, di effetti giuridici specifici riguardanti l'attribuzione, l'integrità, la confidenzialità o il non rifiuto del documento elettronico, anche se, per ovvi motivi, non sarà possibile determinare *a priori* a quali di questi effetti ci si riferisce, con l'obbligo di valutarli sulla base di ogni caso concreto.

**XIV.** Ponendo l'accento su quelle questioni di natura puramente processuale, riguardanti la firma elettronica, e alla luce del nostro ordinamento interno ci troviamo davanti a un panorama generale contraddittorio. Infatti, nell'anno 2000, la LECiv nega indirettamente la natura documentale (e, di conseguenza, il suo carattere di prova documentale) di quello che è un vero *documento*, il *documento elettronico*, evitando questa denominazione e optando per quella di *strumento* (articoli 299.2 e 382 a 384 LECiv). Due anni dopo, nasce l'articolo 24.2 LSSICE, che, rafforzando la nostra teoria, riconosce per la prima volta il carattere di prova documentale del contratto stipulato per via elettronica, che riteniamo ampliata, tuttavia, alla categoria più generale di documento elettronico per il fatto di essere quest'ultima quella che ingloba e integra il primo. In seguito, questa disposizione aggiungerà una seconda comma al primo paragrafo il quale dispone che, quando questi contratti sono firmati elettronicamente, ci si atterrà a quanto previsto nell'articolo 3 LFE, e più nello specifico all'articolo 3.8 LFE, il cui punto iniziale riconosce il valore di prova documentale in giudizio del documento accompagnato da firma elettronica. Nel 2003, nasce la LFE, il cui articolo 3, paragrafi 5-7, definisce per la prima volta nel nostro paese il documento elettronico e riconosce la sua possibile natura di documento pubblico e di documento privato, che avranno il valore e l'efficacia giuridica corrispondente secondo la loro rispettiva natura, e non si riconoscerà apertamente il valore di questo elemento come prova documentale, ma lo farà, invece, per il documento firmato elettronicamente. Quest'anno, come conseguenza dell'entrata in vigore di quest'ultima Legge e senza modificare la sua posizione iniziale, la LECiv include nel suo articolo 326 un terzo paragrafo in cui, ormai, si parla espressamente di documento elettronico, rinviando all'articolo 3 LFE per quei casi in cui la parte interessata alla sua efficacia lo richieda o la sua autenticità venga contestata; e ciò lo fa nel paragrafo riguardante la forza probatoria dei documenti privati senza fare caso al fatto che, proprio in questo articolo 3 LFE, si riconosce altresì la possibile natura pubblica del documento elettronico (articolo 3.5.2º e 6), che non troverà nessuna risposta nella LECiv per il caso in cui la parte interessata alla sua efficacia lo richieda o venga contestata la sua autenticità. Già nel 2014 compare il RIE-SCTE che, per la prima volta, incorpora nell'ordinamento giuridico comunitario il concetto di documento elettronico in un modo molto più adeguato a quanto aveva fatto la LFE, vietando che si possano negare effetti giuridici e ammissibilità come prova in processi giudiziari a un documento elettronico per il semplice fatto di realizzarsi su un supporto fisico diverso dal cartaceo ma comunque adatto per l'archivio di informazione di natura elettronica. Nulla si dice, invece, riguardo al suo possibile valore come prova documentale. Infine, dopo l'entrata in vigore

del Regolamento eIDAS, viene elaborato l' ALSEC (che contempla la deroga della LFE), il cui articolo 3.1.1º riconosce l'esistenza del documento elettronico, ma, incomprensibilmente a causa della tendenza indicata dalla LSSICE e dalla LFE, non si pronuncia in merito all'efficacia processuale di questo, rinviando la questione, invece, alla LECiv e, così, ai problemi di incongruenza indicati, che in nessun momento si cerca di risolvere attraverso il nuovo progetto preliminare; inoltre, il testo non sarà accompagnato da nessuna D. F. che abolisca i riferimenti fatti alla LFE, sia nella LECiv che nella LSSICE, sebbene sostenga la loro integra abrogazione.

A seguito di quest'ultimo rinvio alla LECiv, e tenuto conto della concisione del contenuto dell'articolo 3.1.1º ALSEC, nel caso in cui, finalmente, si promulgherà il testo nei termini esposti, ritorneremmo a una situazione in cui, anche se viene già riconosciuta chiaramente l'esistenza della figura del documento elettronico, non c'è nulla di esplicito riguardo il suo valore come prova documentale. Tuttavia, nell'uso di questa nozione (*documento elettronico*) si riconoscerebbe la sua efficacia processuale generale come prova documentale (anche, di conseguenza, quella del contratto elettronico, già riconosciuto dalla LSSICE); tuttavia, non sarebbe stato male se, ai fini di sicurezza giuridica, fosse stato soppresso qualsiasi riferimento alla nozione di *strumento* dall'articolo 299.2 LECiv e fosse stato riconosciuta, parallelamente, l'esplicita natura e ammissibilità come prova documentale in giudizio dell' documento elettronico, sia come documento pubblico elettronico (articoli 299.1.2º, 317 a 323 e 328 a 334 LECiv) che come documento privato elettronico (articoli 299.1.3º, 324 a 334 LECiv) con o senza firma elettronica.

**XV.** Per il resto, il Regolamento europeo non dice niente riguardo a quello che succede quando determinate proprietà, presumibilmente inerenti i contratti elettronici, vengono contestate in tribunale o quando la parte interessata alla loro efficacia lo richiede. Due sarebbero i possibili scenari.

Un primo scenario, rappresentativo di quei casi in cui il contratto stipulato per via elettronica non dispone di firma elettronica. In questo caso, occorrerebbe per primo determinare se ci troviamo davanti a un contratto elettronico di natura pubblica (la cui analisi non riguarda il nostro campo di studio) o di natura privata. Successivamente, dovremmo analizzare la forza probatoria dei documenti elettronici privati regolata nell'articolo 326 LECiv. Adattata all'ambito elettronico, possiamo soltanto far riferimento alla previsione finale, scritta a modo di guazzabuglio dove si potrebbe includere qualsiasi mezzo di prova

che permetta determinare l'autenticità, l'integrità, la precisione di data e ora o qualsiasi altra caratteristica del documento elettronico, essendo specialmente utile in merito la prova periziale informatica. Ad ogni buon conto, se dal mezzo di prova utilizzabile si ottiene un risultato positivo, si procederà conformemente a quanto prevede il terzo paragrafo dell'articolo 320 LECiv, in modo tale che le spese, i costi e i diritti originati corrispondano esclusivamente a chi abbia formulato la contestazione, e con la possibilità di imporre un'ammenda compresa fra i 120 e i 600€ nel caso in cui quella sia stata temeraria. Nel caso in cui non si possa dedurre l'autenticità, l'integrità, la precisione della data e ora o qualsiasi altra caratteristica del documento elettronico, o nel caso in cui non si sottoponga prova alcuna, il tribunale lo valuterà secondo le regole della sana critica.

L'articolo 326.2 LECiv non dice niente in merito a quei casi in cui si debba determinare la forza probatoria del documento elettronico, non perché sia stato contestato ma perché la parte interessata alla sua efficacia così lo manifesti. Tuttavia, riteniamo che si dovrebbe procedere in modo identico tranne per quanto riguarda il soggetto che debba assumersi le spese, i costi e i diritti originati, che saranno esclusivamente a carico di chi abbia formulato la richiesta di efficacia, non essendo opportuna in questi casi, dal mio punto di vista, alcuna ammenda per temerarietà. Precisamente su questa questione si pronuncia l'articolo 3.1.4º ALSEC, che regola soltanto il caso in cui l'efficacia del documento venga richiesta dalla parte a chi interessa, e ciò lo fa stabilendo, sulla linea di quanto già detto, che la parte che trae beneficio dal documento dovrà assumersi i costi della perizia richiesta; invece, non si pronuncia sui casi di contestazione, che continueranno ad essere disciplinati secondo quanto disposto nella LECiv.

Un secondo scenario, esponente di quei altri casi in cui nel contratto elettronico ci sia la rubrica, anche elettronica. In modo uguale al caso precedente si dovrebbe procedere a determinare, in primo luogo, la natura, pubblica o privata, del contratto firmato elettronicamente e, poi, in secondo luogo, il processo di richiesta di efficacia o di contestazione dell'autenticità, l'integrità, la precisione di data e ora o qualsiasi altra caratteristica del contratto elettronico provato. In ogni caso, se l'aspetto concreto che si contesta all'interno del contratto elettronico è l'autenticità della rubrica con cui sono stati firmati elettronicamente i dati incorporati a questa modalità di documento, occorrerà far riferimento, fino a quando non sarà abrogato, all'articolo 3.8 LFE, precetto che realizza una chiara divisione tra firma elettronica riconosciuta (già qualificata) e firma elettronica avanzata; non si pro-

nuncia invece riguardo alla firma elettronica semplice, che, ai fini di verifica dell'autenticità, verrebbe inclusa, a mio parere, nel processo descritto per questo secondo tipo o modalità di firma. Dal risultato della verifica descritta dipenderà l'autenticità della firma elettronica (anzi, la sua validità ed efficacia, a cui dovremmo aggiungere necessariamente l'autenticità della stessa) e, di conseguenza, l'identificazione autenticata, l'integrità, la confidenzialità e/o non riconoscibilità del contratto elettronico a cui venga incorporata, giacché sono le caratteristiche specifiche che questo SSIisc (secondo la modalità di firma elettronica per cui si opti e la sicurezza che dia) potrebbe garantire.

In caso di abrogazione della LFE dovremmo rivolgerci alla norma incaricata di regolare determinati aspetti dei servizi elettronici di fiducia nel nostro ordinamento giuridico interno come estensione del RIE-SCTE. Questa norma sembra essere rappresentata attualmente dall'ALSEC, il cui articolo 3.1.3º si accontenta di stabilire che nel caso in cui si utilizzi in questi casi una firma elettronica qualificata si supporrà: da un lato, che il documento elettronico raccoglie le caratteristiche messe in discussione; dall'altro, che la firma elettronica è stata prestata in maniera corretta se c'era «[…] nel momento rilevante ai fini della discrepanza», nell'elenco di PSSIisc e SSIisc qualificati regolata negli articoli 22 RIE-SCTE e 19 ALSEC; se poi si richiedesse una perizia *ad hoc*, i costi dovranno essere corrisposti dalla parte che ha richiesto questa relazione. In tal caso, sembra che quello che fa l'articolo 3.1.3º del Progetto Preliminare sia determinare l'effetto di disporre di una firma elettronica qualificata in un documento elettronico contestato o la cui efficacia sia richiesta, senza chiarire se a questo punto si arriva per contestazione previa dell'autenticità e senza indicare cosa succederebbe se la firma elettronica fosse semplice o avanzata.

**XVI.** Per concludere, dobbiamo far attenzione ai soggetti che appartengono alla *struttura triangolare del sistema di firma elettronica*: il firmatario, il terzo che si fida e il PSSIisc.

Con il Regolamento eIDAS, scompare il riferimento a una possibilità specifica prevista nella normativa precedente e che adesso dobbiamo ritenere soppressa. Facciamo riferimento alla possibilità che il firmatario possa essere una persona giuridica, figura che adesso viene sostituita da un'altra finora sconosciuta nel piano normativo: il cosiddetto *creatore di un sigillo*, che esigerà un nuovo adattamento normativo che comporti l'abrogazione implicita di tutti i precetti che non contemplino questa divisione nella LFE.

Inoltre, l'identificazione elettronica, applicata alla firma elettronica, viene definita nel RIE-SCTE come il processo in cui vengono utilizzati i dati di identificazione di una persona in formato elettronico che rappresentano in modo unico una persona fisica o una che rappresenta una persona giuridica; non è prevista, quindi, la possibilità che una persona fisica possa rappresentare un'altra persona fisica (nemmeno che una persona giuridica possa rappresentare un'altra persona giuridica, una circostanza che, per quanto complessa, sarebbe in pratica fattibile), una opzione espressamente prevista nelle nozioni di firmatario del RDLFE, della DFE e della LFE. Questo problema sembra risolversi nel nostro paese tramite l'articolo 5.1.a) ALSEC, che, nell'alludere all'estinzione della validità dei certificati elettronici attraverso revoca, dispone espressamente che questa possa avere luogo, tra le altre, per la «[r]ichiesta formulata dal firmatario, la persona fisica o giuridica rappresentata da questo, un terzo autorizzato, il creatore del sigillo o il titolare del certificato di autenticazione del sito web», prevedendo, pur indirettamente, questa possibilità e contraddicendo, di conseguenza, quello che la norma comunitaria attuale non prevede in modo esplicito, sebbene ciò ci sembri quantomeno incomprensibile. Per questo motivo, sarebbe più adeguata, oltre all'eventuale promulgazione in Spagna di quello che per il momento è un Progetto Preliminare, la modifica del RIE-SCTE in merito a questo punto concreto, aggiungendo ai paragrafi 1), 3) e 4) dell'articolo 3 questa ampliazione nei casi di rappresentazione con delle definizioni che potrebbero essere quelle che seguono:

*1) "identificazione elettronica": processo per il quale si utilizzano dati identificativi di una persona in formato elettronico che rappresentano in modo unico una persona fisica o giuridica, una persona fisica che rappresenta una persona giuridica o un'altra persona fisica o una persona giuridica che rappresenta una persona fisica oppure un'altra persona giuridica"*

*2) "dati di identificazione elettronica della persona": insieme di dati che permettono di stabilire l'identità di una persona fisica o giuridica, di una persona fisica che rappresenta una persona giuridica o un'altra persona fisica o una persona giuridica che rappresenta una persona fisica oppure un'altra persona giuridica"*

*3) "sistema di identificazione elettronica": regime per l'identificazione elettronica in virtù del quale vengono rilasciati mezzi di identificazione elettronica alle persone fisiche o giuridiche, alle persone fisiche che rappresentano persone giuridiche o altre persone fisiche o a persone giuridiche che rappresentano persone fisiche oppure altre persone giuridiche.*

Infine, e all'interno della dinamica propria del contratto elettronico, dobbiamo rendere noto un fatto ovvio ma, allo stesso tempo, rilevante. Facciamo riferimento alla possibilità che il firmatario assuma così il ruolo del PSSI come quello del DSSI; di conseguenza, e secondo il caso, ci dovremmo rivolgere a tutto quanto esposto rispetto all'uno o all'altro nel corso di questa ricerca, essendo di applicazione cumulativa i diritti, gli obblighi e le responsabilità generali proprie della parte attiva o passiva del contratto elettronico, insieme a quelle altre specifiche proprie della sua condizione di firmatario del suddetto documento, ciascuna delle quali sembrano rispecchiate e ben separate in queste pagine. La stessa cosa succederà con la figura di terzi che si fidano della firma elettronica del firmatario.

# BIBLIOGRAFÍA


ADIEGO RODRÍGUEZ, J., «Problemática informática de la protección de obras digitales protegidas», en Mata y Marín, R.M., Javato Martín, A.M. (coords.) *La propiedad intelectual en la era digital: límites e infracciones a los derechos de autor en Internet*, Las Rozas, La Ley, 2011, pp. 25 a 62.

ADSUARA VARELA, B., «Algunas consideraciones previas sobre el comercio electrónico», *Información comercial española*, vol. 813, 2004, pp. 15 a 26.

ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autentificación de los ciudadanos», en Gamero Casado, E. (coord.) *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, Valencia, Tirant lo Blanch, 2017, pp. 679 a 772.

ALAMILLO DOMINGO, I., «Los servicios de confianza y la prueba electrónica», en Oliva León, R., Valero Barceló, S. (coords.) *La prueba electrónica: validez y eficacia procesal*, Juristas con futuro, 2016, pp. 144 a 151.

ALAMILLO DOMINGO, I., «Tipología legal de la firma electrónica en la Unión Europea», *Revista de la contratación electrónica*, vol. 23, 2002, pp. 19 a 42.

ALAMILLO DOMINGO, I.; RUBIO VELÁZQUEZ, R., «Firma electrónica y certificación digital», en AA.VV. (coord.) *Internet: claves legales para la empresa*, Madrid, Civitas, 2002, pp. 101 a 177.

ALAMILLO DOMINGO, I.; URIOS APARISI, X., «Comentario crítico de la Ley 59/2003, de 19 de diciembre, de firma electrónica», *Revista de la contratación electrónica*, vol. 46, 2004, pp. 3 a 64.

ALBA, M., «Order out of chaos: technology, intermediation, trust and reliability as the basis for the recognition of legal effects in electronic transactions», *Creighton University law*

*review*, vol. 47, 2014, pp. 387 a 521.

ALCOVER GARAU, G., «Concepto de firma electrónica, firma electrónica y firma manual», en Perales Sanz, J.L. (coord.) *La seguridad jurídica en las transacciones electrónicas: Seminario organizado por el Consejo General del Notariado en el UIMP*, Madrid, Civitas, 2002, pp. 31 a 46.

ALCOVER GARAU, G., «El Real Decreto-ley sobre la firma electrónica», *Revista de la contratación electrónica*, vol. 1, 2000, pp. 7 a 27.

ALCOVER GARAU, G., «La firma electrónica como medio de prueba», *Cuadernos de Derecho y comercio*, vol. 13, 1994, pp. 11 a 42.

ALCOVER GARAU, G.; ALONSO UREBA, A., «La firma electrónica», en De Ros Cerezo, R.M., Cendoya Méndez de Vigo, J.M. (coords.) *Derecho de Internet : la contratación electrónica y firma digital*, Cizur Menor, Aranzadi, 2000, pp. 175 a 206.

ALFARO ÁGUILA-REAL, J.; PAZ-ARES RODRÍGUEZ, J. C., *Las condiciones generales de la contratación: estudio de las disposiciones generales*, Madrid, Civitas, 1991.

ALFONSO SÁNCHEZ, I. R., «La sociedad de la información, sociedad del conocimiento y sociedad del aprendizaje. Referentes en torno a su formación», *Bibliotecas. Anales de investigación*, vol. 2, 2016, pp. 235 a 243.

ALMAGRO NOSETE, J., *Derecho procesal*, Valencia, Tirant lo Blanch, 1996.

ALMONACID LAMELAS, V.; ALAMILLO DOMINGO, I., «La fe pública electrónica en el procedimiento local: de la "fehaciencia" electrónica automatizada al nuevo ejercicio de la función reservada de fe pública», en Campos Acuña, M.C. (coord.) *El nuevo procedimiento administrativo local tras la Ley 39/2015*, Las Rozas, Wolters Kluwer, 2016, pp. 425 a 448.

ALMONACID LAMELAS, V.; ALAMILLO DOMINGO, I., «Los ciudadanos en el procedimiento y su personalidad electrónica: medios de identificación y firma», en Campos Acuña, M.C. (coord.) *El nuevo procedimiento administrativo local tras la Ley 39/2015*, Las Rozas, Wolters Kluwer, 2016, pp. 193 a 233.

ALONSO CONDE, A. B., *Comercio electrónico: antecedentes, fundamentos y estado actual*, Madrid,

Dykinson, 2004.

ÁLVAREZ SAAVEDRA, F. J., *Diccionario de criminalística. Los secretos de las investigaciones de la policía científica*, Barcelona, Planeta, 2003.

AMAR RODRÍGUEZ, V. M., «La interculturalidad tecnológica: inforricos e infopobres», en AA.VV. (coord.) *Inmigración, interculturalidad y convivencia*, Ceuta, Instituto de Estudios Ceutíes, 2002, pp. 363 a 370.

APARICIO VAQUERO, J. P., «Los consumidores y sus relaciones con los proveedores de servicios de la sociedad de la información», *Revista de la contratación electrónica*, vol. 89, 2008, pp. 3 a 65.

APARICIO VAQUERO, J. P.; MORO ALMARAZ, M. J.; BATUECAS CALETRÍO, A., *Internet y comercio electrónico*, Salamanca, Universidad de Salamanca, 2002.

ARIAS POU, M., «El deber de información en la contratación electrónica», *La ley mercantil*, vol. 17, 2015, pp. 3 a 10.

ARIAS POU, M., *Manual práctico de comercio electrónico*, Las Rozas, La Ley, 2006.

ASENCIO MELLADO, J. M., *Derecho procesal civil*, Valencia, Tirant lo Blanch, 2015.

BARIATTI, S., «Internet: aspects rélatifs aux conflits de lois», *Rivista di Diritto internazionale privato e processuale*, vol. 550, 1997, pp. 545 a 556.

BARLOW, J. P., «A declaration of the independence of cyberspace», 1996, Davos.

BARNES VÁZQUEZ, J., «La Internet y el Derecho: una nota acerca de la libertad de expresión e información en el espacio cibernético», *Cuadernos de Derecho judicial*, vol. 6, 1997, pp. 235 a 241.

BARREIROS FERNÁNDEZ, J., «El papel del notariado en el uso de la firma digital», *Notariado y contratación electrónica*, vol. 1, 2000, pp. 7 a 26.

BARRIUSO RUIZ, C., *La contratación electrónica*, Madrid, Dykinson, 1998.

BATUECAS CALETRÍO, A., «Hacia una ley de firma electrónica que mejore el Real Decreto-ley de firma electrónica 14/1999, de 17 de septiembre», en Aparicio Vaquero, J.P., Moro

Almaraz, M.J., Batuecas Caletrío, A. (coords.) *Internet y comercio electrónico*, Salamanca, Universidad de Salamanca, 2002, pp. 153 a 176.

BAUZÁ MARTORELL, F. J., «Las notificaciones telemáticas como fórmula de modernización de la oficina judicial», en AA.VV. (coord.) *Estudios acerca de la reforma de la justicia en España*, Madrid, Real Academia de Jurisprudencia y Legislación y Ministerio de Justicia, 2004, pp. 463 a 477.

BEAUPÉRIN, T., «Think small first in the EU?: a reality check», *Eurochambres report on the European Commission's application of the SME Test*, vol. 5, 2014, pp. 93 a 96.

BELL, D., *The coming of post-industrial society: a venture in social forecasting*, Nueva York, Basic Books, 1976.

BENTHAM, J., *Rationale of judicial evidence: specially applied to English practice*, Londres, Manuscrito, 1827.

BERCOVITZ RODRÍGUEZ-CANO, A., *Apuntes de Derecho mercantil: Derecho mercantil, Derecho de la competencia y propiedad industrial*, Cizur Menor, Aranzadi, 2011.

BERROCAL LANZAROT, A. I., «La firma electrónica y su regulación en la Ley 59/2003, de 19 de diciembre, de firma electrónica», *Foro: revista de ciencias jurídicas y sociales*, vol. 3, 2006, pp. 397 a 465.

BESCÓS TORRES, M., «Formas contractuales en el comercio electrónico», *Información comercial española*, vol. 813, 2004, pp. 173 a 186.

BETTI, E., *Teoria generale del negozio giuridico*, Turín, Utet Giuridica, 1952.

BLANCO URZÁIZ, J., «Sistema de tutela y gestión de los certificados digitales al amparo de la nueva Ley de firma electrónica», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 6, 2004, pp. 101 a 110.

BOBBIO, N., *Diccionario de política*, México D. F., Sigo XXI, 1976.

BOBBIO, N., *Teoria dell'ordinamento giuridico*, Turín, Giappichelli, 1957.

BOLÁS ALFONSO, J., «Firma electrónica, comercio electrónico y fe pública notarial», *Revista jurídica del notariado*, vol. 36, 2000, pp. 31 a 64.

BONARDELL LENZANO, R., «La firma electrónica: especial consideración de sus efectos jurídicos», *Notariado y contratación electrónica*, vol. 1, 2000, pp. 55 a 70.

BONARDELL LENZANO, R., «La seguridad jurídica en las transacciones electrónicas», *Anales de la academia matritense del notariado*, vol. 43, 2005, pp. 133 a 174.

BOSS, A.; RITTER, J. B., *Electronic Data Interchange agreements: a guide and sourcebook*, París, International chamber of commerce, 1993.

BOTANA GARCÍA, G. A., «Noción de comercio electrónico», en Botana García, G.A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 5 a 62.

BOWREY, K., *Law & Internet cultures*, Cambridge, Cambridge University Press, 2005.

BRAVO, F., *Contrattazione telematica e contrattazione cibernetica*, Milán, Giuffrè, 2007.

BRAZELL, L., «Electronic security: encryption in the real world», *European intellectual property review*, vol. 21, 1999, pp. 17 a 27.

BRIZ ESCRIBANO, J.; LASO BALLESTEROS, I., *Internet y comercio electrónico: características, estrategias, desarrollo y aplicaciones*, Madrid, Mundi Prensa Libros, 2000.

BUONOMO, G., «Lo schema governativo stravolge il processo civile», *InterLwx*, vol. 1, 2002, pp. 1 a 3.

BUONOMO, G.; MERONE, A., «La scrittura privata informatica: firme elettroniche, valore probatorio e disconoscimento in giudizio (alla luce delle modifiche introdotte dalla l. 221/2012)», *Judicium: il processo civile in Italia e in Europa*, vol. 1, 2013, pp. 1 a 33.

BURNSTEIN, M. R., «Conflicts on the net: choice of Law in transactional cyberspace», *Vanderbilt journal of transactional Law*, vol. 29, 1996, pp. 75 a 90.

BUSTO LAGO, J. M., «La responsabilidad civil de los prestadores de servicios de intermediación en la sociedad de la información», *Actualidad jurídica Aranzadi*, vol. 54, 2002, pp. 1 a 6.

CABANELLAS DE LAS CUEVAS, G., *Derecho de Internet*, Buenos Aires, Elisa, 2012.

CACHAFEIRO GARCÍA, F.; GARCÍA PÉREZ, R., «No sujeción a autorización previa de la

prestación de servicios de la sociedad de la información (comentario al art. 6 de la LSSICE)», *Revista de la contratación electrónica*, vol. 45, 2004, pp. 39 a 56.

CALVO CARAVACA, A.; CASRRASCOSA GONZÁLEZ, J., *Conflictos de leyes y conflictos de jurisdicción en Internet*, Madrid, Colex, 2001.

CAMACHO CLAVIJO, S., *Partes intervinientes, formación y prueba del contrato electrónico*, Madrid, Reus, 2005.

CAMMARATA, M.; MACCARONE, E., *La firma digitale sicura. Il documento informatico nell'ordinamento italiano*, Milán, Giuffrè, 2003.

CAMPILLOS GONZÁLEZ, G. M., «La Ley de servicios de la sociedad de la información: marco jurídico de las actividades económicas a través de Internet», *Economía industrial*, vol. 338, 2001, pp. 51 a 58.

CARBAJO CASCÓN, F., «Aspectos sustantivos del procedimiento administrativo para la salvaguarda de derechos de propiedad intelectual en Internet», *IDP: revista de Internet, Derecho y Política*, vol. 15, 2012, pp. 7 a 16.

CARLONI, E., «Tendenze recenti e nuovi principi della digitalizzazione pubblica», *Giornale di Diritto amministrativo: mensile di legislazione, giurisprudenza, prassi e opinioni*, vol. 2, 2015, pp. 148 a 158.

CARNELUTTI, F., *La prova civile: parte generale. Il concetto giuridico della prova*, Milán, Giuffrè, 1992.

CARO BEJARANO, M. J., «Peligros tecnológicos», *Cuadernos de estrategia*, vol. 159, 2013, pp. 183 a 227.

CARRASCOSA LÓPEZ, V., «Valor probatorio del documento electrónico», *Informática y Derecho: revista iberoamericana de Derecho informático*, vol. 8, 1995, pp. 133 a 174.

CARRETERO PÉREZ, J., *Descubre Internet*, Madrid, Prentice Hall, 2001.

CASTELLS OLIVÁN, M., *La era de la información: economía, sociedad y cultura*, Madrid, Alianza, 1997.

CASTELLS OLIVÁN, M., *La galaxia Internet: reflexiones sobre Internet, empresa y sociedad*, Barcelona, Plaza & Janés, 2001.

CASTELLS OLIVÁN, M., *The power of identity*, Oxford, Wiley-Blackwell, 2010.

CAVALLONI, A., *Il contratto telematico: profili generali*, Padua, Cedam, 2013.

CAVANILLAS MÚGICA, S., «Dieciocho recomendaciones para la empresa que practique comercio electrónico con consumidores», *Actualidad informática Aranzadi: revista de informática para juristas*, vol. 37, 2000, pp. 1 a 6.

CAVANILLAS MÚGICA, S.; JULIÀ BARCELÓ, R., «La responsabilidad civil por daños causados a través de Internet», en Sala Arquer, J.M., Martínez-Simancas Sánchez, J. (coords.) *Derecho sobre Internet*, Madrid, Banco Santander Central Hispano, 2008, pp. 267 a 291.

CAVANILLAS MÚGICA, S.; PAYERAS CAPELLÁ, M. M., «Los servidores de acceso y alojamiento: descripción técnica y legal», en Cavanillas Múgica, S. (coord.) *Deberes y responsabilidades de los servidores de acceso y alojamiento: un análisis multidisciplinar*, Granada, Comares, 2005, pp. 1 a 28.

CENDOYA MÉNDEZ DE VIGO, J. M., «La protección de los consumidores», en De Ros Cerezo, R.M., Cendoya Méndez de Vigo, J.M. (coords.) *Derecho de Internet: la contratación electrónica y firma digital*, Cizur Menor, Aranzadi, 2000, pp. 123 a 142.

CIACCI, G., *La firma digitale*, Milán, Il Sole 24 Ore, 2000.

CLARIZIA, R., *I contratti informatici*, Milanofiori Assago, Utet Giuridica, 2007.

CLEMENTE MEORO, M. E., «Algunas consideraciones sobre la contratación electrónica», *Revista Aranzadi de Derecho patrimonial*, vol. 4, 2000, pp. 59 a 86.

COGLIOLO, P., *Filosofia del Diritto privato*, Florencia, Barbera, 1891.

COMANDÉ, G.; SICA, S., *Il commercio elettronico: profili giuridici*, Turín, Giappichelli, 2001.

COMISIÓN EUROPEA, *Europa y la sociedad global de la información. Recomendaciones al Consejo Europeo*, Bruselas, 1994.

CONFERENCIA DE LA HAYA DE DERECHO INTERNACIONAL PRIVADO, *Electronic commerce and international jurisdiction*, 2000.

CORDÓN GARCÍA, J. A.; ALONSO ARÉVALO, J.; GÓMEZ DÍAZ, R.; LÓPEZ LUCAS, J., *Las nuevas*

*fuentes de información: información y búsqueda documental en el contexto de la Web 2.0*, Madrid, Pirámide, 2012.

CREMADES GARCÍA, J.; GONZÁLEZ MONTES, J. L., *La nueva Ley de Internet: comentarios a la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Las Rozas, La Ley-Actualidad, 2003.

CRUZ RIVERO, D., «El DNI electrónico y el mercado de entidades de certificación», *Revista de la contratación electrónica*, vol. 69, 2006, pp. 21 a 56.

CRUZ RIVERO, D., *La firma electrónica reconocida: análisis de los requisitos del artículo 3.3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica*, Madrid, Consejo General del Notariado, 2006.

CRUZ RIVERO, D., «Las definiciones de firma electrónica en el Real Decreto-ley 14/1999, sobre firma electrónica, y el Proyecto de Ley de firma electrónica», en Davara Rodríguez, M.Á. (coord.) *XVIII Encuentros sobre Informática y Derecho, 2003-2004*, Madrid, Universidad Pontificia de Comillas, 2004, pp. 121 a 136.

DAHM, W., *Deutsches recht*, Stuttgart, Kohlhammer, 1951.

DAVARA RODRÍGUEZ, M. Á., «El documento electrónico, informático y telemático y la firma electrónica», *Actualidad informática Aranzadi: revista de informática para juristas*, vol. 24, 1997, pp. 3 a 15.

DAVARA RODRÍGUEZ, M. Á., «La liberalización del mercado de las telecomunicaciones: una perspectiva desde la ética», en Pinto Monteiro, A. (coord.) *As telecomunicaçoes e o Direito na sociedade da Informaçao*, Coimbra, Instituto jurídico da comunicaçao, Faculdade de Direito, Universidade de Coimbra, 1999, pp. 395 a 405.

DAVARA RODRÍGUEZ, M. Á., *Manual de Derecho informático*, Cizur Menor, Aranzadi, 2015.

DE CASTRO Y BRAVO, F., *El negocio jurídico*, Madrid, Civitas, 1967.

DE LA OLIVA SANTOS, A., *Derecho procesal civil*, Madrid, Centro de estudios Ramón Areces, 1995.

DE LA RICA, E., *Marketing en Internet y e-business*, Madrid, Anaya, 2000.

DE LOS MOZOS Y DE LOS MOZOS, J. L., «La forma del negocio jurídico», *Anuario de Derecho civil*, vol. 4, 1968, pp. 745 a 778.

DE MIGUEL ASENSIO, P. A., *Caracterización y organización de Internet: perspectiva jurídica*, Cizur Menor, Aranzadi, 2015.

DE MIGUEL ASENSIO, P. A., *Contratación electrónica*, Cizur Menor, Aranzadi, 2015.

DE MIGUEL ASENSIO, P. A., *Derecho privado de Internet*, Madrid, Civitas, 2001.

DE MIGUEL ASENSIO, P. A., «Regulación de la firma electrónica: balance y perspectivas», *Direito da sociedade da informaçao*, vol. 5, 2004, pp. 115 a 143.

DE MURI, L., «Gli aspetti legali e contrattuali del commercio telematico», en AA.VV. (coord.) *Commercio elettronico*, Milanofiori Assago, Wolters Kluwer, 2014, pp. 7 a 23.

DE ROSELLÓ MORENO, R., *El comercio electrónico y la protección de los consumidores*, Barcelona, Cedecs, 2001.

DEL PESO NAVARRO, E., *Servicios de la sociedad de la información: comercio electrónico y protección de datos*, Madrid, Díaz de Santos, 2003.

DELACOURT, J. T., «The international impact of Internet regulation», *Harvard international law journal*, vol. 38, 1997, pp. 207 a 235.

DELFINI, F., *Contratto telematico e commercio elettronico*, Milán, Giuffrè, 2002.

DELFINI, F., *Il commercio elettronico*, Milán, Egea, 1999.

DEVIS ECHANDÍA, H., *Teoría general de la prueba judicial*, Buenos Aires, Zavalía, 1970.

DI COCCO, C.; SARTOR, G., *Temi di Diritto dell'informatica*, Turín, Giappichelli, 2013.

DÍAZ DUMONT, J. R., *Tecnologías de información y comunicación e inclusión social: estudio científico*, Múnich, Grin, 2015.

DÍAZ FRAILE, J. M., «Comentarios a la Directiva y al Proyecto de Ley español de comercio electrónico de 2000: contenido y proceso de elaboración», *Revista crítica de Derecho inmobiliario*, vol. 663, 2001, pp. 81 a 122.

DÍAZ FRAILE, J. M., «El comercio electrónico: Directiva y Proyecto de ley español de 2000. Crónica de su contenido, origen, propósitos y proceso de elaboración», *Actualidad civil*, vol. 1, 2001, pp. 31 a 58.

DÍAZ FRAILE, J. M., «El comercio electrónico: Directiva y Proyecto de Ley español de 2000. Crónica de su contenido, origen, propósitos y proceso de elaboración», *Actualidad civil*, vol. 1, 2001, pp. 31 a 58.

DÍAZ FRAILE, J. M., «El documento electrónico y la firma digital: su regulación en la Unión Europea», *Noticias de la Unión Europea*, vol. 177, 1999, pp. 9 a 30.

DÍAZ FRAILE, J. M., «Estudio de la regulación de la firma electrónica en la directiva europea de 13 de mayo de 1998», *La ley: revista jurídica española de doctrina, jurisprudencia y bibliografíaL*, vol. 6, 1998, pp. 2149 a 2162.

DÍAZ MORENO, A., «Certificados de clave pública y entidades de certificación», en Perales Sanz, J.L. (coord.) *La seguridad jurídica en las transacciones electrónicas: seminario organizado por el Consejo General del Notariado en el UIMP*, Madrid, Civitas, 2002, pp. 81 a 108.

DÍAZ MORENO, A., «Concepto y eficacia de la firma electrónica en la Directiva 1999/93/CE, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica», *Revista de la contratación electrónica*, vol. 2, 2000, pp. 3 a 51.

DOMÍNGUEZ LUELMO, A., «La contratación electrónica y la defensa del consumidor», en Echebarría Sáenz, J.A. (coord.) *El comercio electrónico*, Madrid, Edisofer, 2001, pp. 31 a 80.

DOWNES, L.; CUI, C., *Estrategias digitales para dominar el mercado*, Barcelona, Granica, 1999.

DREYZIN DE KLOR, A., «Derecho aplicable al comercio electrónico», *Seqüência: estudios jurídicos e políticos*, vol. 50, 2005, pp. 273 a 300.

DRUCKER, P., *The age of discontinuity: guidelines to our changing society*, Nueva York, Harper & Row, 1969.

DYSON, E.; GILDER, G.; KEYWORTH, G.; TOFFLER, A., «Cyberspace and the american dream: a magna carta for the knowledge age», *The information society*, vol. 12, pp. 295 a 308.

EBERSBACH, A.; GLASER, M.; HEIGL, R., *Social Web*, Constanza, Uvk Verlagsgesellschaft, 2008.

ECHEBARRÍA SÁENZ, J. A., *El comercio electrónico*, Madrid, Edisofer, 2001.

ECHEVERRÍA EZPONDA, J., «21 tesis sobre el tercer entorno, Telépolis y la vida cotidiana», *XIV Congreso de estudios vascos*, vol. 14, 1998, pp. 7 a 11.

ECHEVERRÍA EZPONDA, J., *Los señores del aire: telépolis y el tercer entorno*, Barcelona, Destino, 1999.

ELÍAS BATURONES, J. J., *La prueba de documentos electrónicos en los tribunales de justicia*, Valencia, Tirant lo Blanch, 2008.

ELOSUA DE JUAN, M., *Diccionario LID. Comunicación y marketing*, Madrid, Lid, 2004.

ESCOBAR ESPINAR, M., *El comercio electrónico: perspectiva presente y futura en España*, Madrid, Fundación Retevisión, 2000.

FADDA, S., «L'Electronic Data Interchange nella normativa italiana e straniera», *Rivista dell'informazione e dell'informatica*, vol. 1, 1994, pp. 91 a 117.

FELIÚ ÁLVAREZ DE SOTOMAYOR, S., *La contratación internacional por vía electrónica con participación de consumidores: la elección entre la vía judicial y la vía extrajudicial en la resolución de conflictos*, Granada, Comares, 2006.

FERNÁNDEZ DOMINGO, J. I., *Algunas notas acerca de la contratación y el comercio electrónico*, Valencia, Tirant lo Blanch, 2003.

FERNÁNDEZ DOMINGO, J. I., «La contratación electrónica y el Real Decreto-ley 14/1999 sobre firma electrónica», *Actualidad civil*, vol. 2, 2000, pp. 527 a 548.

FERNÁNDEZ DOMINGO, J. I., *La firma electrónica: aspectos de la Ley 59/2003, de 19 de diciembre*, Madrid, Reus, 2006.

FERNÁNDEZ ESTEBAN, M. L., «Limitaciones constitucionales e inconstitucionales a la libertad de expresión en Internet», *Revista española de Derecho constitucional*, vol. 53, 1998, pp. 283 a 311.

FERRER GOMILA, J. L.; MARTÍNEZ NADAL, A., «El problema temporal del sistema de certificados en el comercio electrónico», *Revista de la contratación electrónica*, vol. 1, 2000, pp. 29 a 47.

FERRI, G. B., «Forma e autonomia negoziale», *Quadrimestre*, vol. 1, 1987, pp. 305 a 323.

FINOCCHIARO, G. D., «Ancora novità legislative in materia di documento informatico: le recenti modifiche al Codice dell'amministrazione digitale», *Contratto e impresa*, vol. 2, 2011, pp. 495 a 511.

FINOCCHIARO, G. D., «Documento informatico e firma digitale», *Contratto e impresa*, vol. 2, 1998, pp. 956 a 971.

FINOCCHIARO, G. D., «La firma digitale: formazione, archiviazione e trasmissione di documenti con strumenti informatici e telematici», en F., G. (coord.) *Commentario del Codice civile Scialoja-Branca*, Bolonia, Zanichelli, 2000, pp. 2699 a 2720.

FINOCCHIARO, G. D., «Le copie per immagine su supporto informatico avranno l'efficacia probatoria degli atti originali», *Guida al Diritto*, vol. 8, 2011, p. 62 a 75.

FINOCCHIARO, G. D., «Una prima lettura del Reg. UE n. 910/2014 (c.d. eIDAS): identificazione on line, firme elettroniche e servizi fiduciari», *Le nuove leggi civili commentate*, vol. 3, 2015, pp. 419 a 428.

FINOCCHIARO, G. D.; DELFINI, F., *Diritto dell'informatica*, Milanofiori Assago, Utet Giuridica, 2007.

FIORELLI, G. I., *Il contratto elettronico tra armonizzazione materiale e Diritto internazionale privato*, Padua, Cedam, 2006.

FORCADA MIRANDA, F. J., «El registro de la propiedad y las nuevas tecnologías: la publicidad formal, acceso al proceso y efectos jurídicos», *Estudios de Derecho judicial*, vol. 43, 2002, pp. 85 a 143.

FORO DE DAVOS, *Consejo para la Agenda Global*, 2013.

GALINDO AYUDA, F., «Comentarios al Borrador de Anteproyecto de Ley de firma electrónica», *La ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*, vol. 2, 2002, pp. 1748 a 1751.

GÁLLEGO HIGUERAS, G. F., «Comentarios a la reciente Ley 59/2003, de 19 de diciembre, de firma electrónica: algunas novedades al marco regulador existente», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 6, 2004, pp. 21 a 40.

GALLEGO PEREIRA, M. D.; BUENO ÁVILA, S.; LÓPEZ JIMÉNEZ, D., *La Web 2.0: una visión empresarial y jurídica*, Cizur Menor, Aranzadi, 2014.

GÁMIR, A., «Los procesos de cambio en los servicios personales y el comercio: autoservicio, telecompra y teleservicio», *Boletín de la asociación de geógrafos españoles*, vol. 24, 1997, pp. 13 a 28.

GARCÍA AGUILAR, N., «El Real Decreto-ley 14/1999 sobre firma electrónica», *Revista internauta de práctica jurídica*, vol. 4, 2000, pp. 1 a 16.

GARCÍA ARETIO, L., *De la educación a distancia a la educación virtual*, Barcelona, Ariel, 2007.

GARCÍA COSO, E., «La Unión Europea y los operadores de telecomunicaciones», en Botana García, G.A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 109 a 156.

GARCÍA DE ENTERRÍA MARTÍNEZ-CARANDE, E., *Justicia y seguridad jurídica en un mundo de leyes desbocadas*, Madrid, Civitas, 1999.

GARCÍA DEL POYO, R.; MARTÍNEZ ROJAS, S., «La responsabilidad de los intermediarios», en Pérez Bes, F. (coord.) *El Derecho de Internet*, Barcelona, Atelier, 2016, pp. 225 a 252.

GARCÍA MÁS, F. J., «Algunos aspectos de la ley de servicios de la sociedad de la información: el comercio electrónico, un reto de presente y de futuro. Especial consideración de la contratación electrónica», *Revista jurídica del notariado*, vol. 55, 2005, pp. 73 a 120.

GARCÍA MÁS, F. J., *Comercio y firma electrónicos: análisis jurídico de los servicios de la sociedad de la información*, Valladolid, Lex Nova, 2002.

GARCÍA MÁS, F. J., «El documento público electrónico (1)», en Escolano Navarro, J.J. (coord.) *Nuevas tecnologías en la contratación, sociedad nueva empresa e hipoteca electrónica : seminario organizado por el Consejo General del Notariado en la UIMP en julio de 2003*, Madrid, Civitas, 2005, pp. 107 a 145.

GARCÍA MÁS, F. J., «La contratación electrónica: la firma y el documento electrónicos», *Revista crítica de Derecho inmobiliario*, vol. 652, 1999, pp. 765 a 790.

GARCÍA MÁS, F. J., «La firma electrónica Directiva 1999/93/CE, de 13 de diciembre de 1999 y Real Decreto-ley 14/1999 de 17 de septiembre», *Notariado y contratación electrónica*, vol. 1, 2000, pp. 95 a 138.

GARCÍA MÁS, F. J.; LÓPEZ-MONÍS GALLEGO, A., «La contratación electrónica: modernidad y seguridad jurídica», en F., D. de M.J. (coord.) *Instituciones de Derecho privado*, Madrid, Civitas, 2004, pp. 110 a 165.

GARCÍA MEXÍA, P., *Derecho europeo de Internet: hacia la autonomía académica y la globalidad geográfica*, Oleiros, Netbiblo, 2009.

GARCÍA MEXÍA, P., «El Derecho de Internet», en Pérez Bes, F. (coord.) *El Derecho de Internet*, Barcelona, Atelier, 2016, pp. 17 a 39.

GARCÍA VIADA, C.; GOMÁ LANZÓN, F., «Libro blanco de la firma electrónica notarial», *Revista jurídica del notariado*, vol. 45, 2003, pp. 269 a 313.

GAUTRAIS, V.; LEFEBVRE, G.; BENYEKHLEF, K., «Droit du commerce électronique et normes applicables: l'emergence de la lex electronica», *Revue de Droit des affaires internationales*, vol. 5, 1997, pp. 547 a 583.

GENOVESE, A., *Le forme volontarie nella teoria dei contratti*, Padua, Cedam, 1949.

GERBOLÉS RODRÍGUEZ, S., «Comentario a los artículos 27, 28 y 29», en Cremades García, J., González Montes, J.L. (coords.) *La nueva ley de Internet: comentarios a la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*, Las Rozas, La Ley, 2003, pp. 427 a 444.

GIBSON, W., *Johnny Mnemonic*, Nueva York, Ace Books, 1982.

GIBSON, W., *Neuromancer*, Nueva York, Ace Books, 1984.

GIGANTE, A., «Blackhole in cyberspace: the legal void in the Internet», *The John Marshall journal of computer & information Law*, vol. 3, 1997, pp. 413 a 436.

GOMES SOARES, F. S., «La prueba en la contratación electrónica de consumo», *Riedpa: revista*

*de estudios sobre Derecho procesal y arbitraje*, vol. 3, 2009, pp. 1 a 28.

GÓMEZ DE LIAÑO GONZÁLEZ, F., *El proceso civil*, Oviedo, Forum, 1990.

GÓMEZ GÓMEZ, A.; PUENTE GARCÍA, F. J.; MITRE ARANDA, M., «Importancia del comercio electrónico y su incidencia en la logística de aprovisionamientos», *Ingeniería industrial*, vol. 2, 2004, pp. 46 a 53.

GÓMEZ LOZANO, M. M., «Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 199», *Ars iuris Salmanticensis: revista europea e iberoamericana de pensamiento y análisis de Derecho, Ciencia, Política y Criminología*, vol. 1, 2015, pp. 267 a 269.

GÓMEZ VIEITES, Á. M.; CEREJIDO SAMOS, I.; VELOSO ESPIÑERA, M., *Economía digital y comercio electrónico*, Santiago de Compostela, Tórculo Edicións, 2002.

GONZÁLEZ-ECHENIQUE CASTELLANOS DE UBAO, L., «Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre firma electrónica», en De Ros Cerezo, R.M., Cendoya Méndez de Vigo, J.M. (coords.) *Derecho de Internet : la contratación electrónica y firma digital*, 2000, pp. 207 a 260.

GONZÁLEZ-ECHENIQUE CASTELLANOS DE UBAO, L., «La firma electrónica», en AA.VV. (coord.) *Derecho de Internet: la Ley de servicios de la sociedad de la información y de comercio electrónico*, Cizur Menor, Aranzadi, 2003, pp. 611 a 674.

GONZÁLEZ DE ALAIZA CARDONA, J. J.; PERTÍÑEZ VÍLCHEZ, F., «Los contratos de adhesión y la contratación electrónica», en Bercovitz Rodríguez-Cano, R., Moralejo Imbernón, N.I., Quicios Molina, M.S. (coords.) *Tratado de los contratos*, Valencia, Tirant lo Blanch, 2013, pp. 1791 a 2004.

GONZÁLEZ DE LA GARZA, L. M., *Comunicación pública en Internet*, Madrid, Creaciones Copyright, 2004.

GONZÁLEZ GRANDA, P., «Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico», *Indret: revista para el análisis del Derecho*, vol. 4, 2007, pp. 1 a 36.

GONZÁLEZ MORENO, M., «¿Qué se ha de tener en cuenta a la hora de implantar servicios de

identificación y firma electrónica?», *Actualidad jurídica Aranzadi*, vol. 923, 2016, pp. 1 y 2.

GONZÁLEZ NAVARRO, F., «Comentario al art. 45 de la Ley de régimen jurídico de las Administraciones públicas y procedimiento administrativo común», *Estudios y comentarios legislativos (Civitas)*, vol. 1, 2007, pp. 1 a 49.

GONZÁLEZ ROBLES, A.; POHLMANN, N.; ENGLING, C.; JÄGER, H.; ERNST, E., «Doubtless identification and privacy preserving of user in cloud systems», en Pohlmann, N., Reimer, H., Schneider, W. (coords.) *Securing electronic business processes*, Berlín, Springer, 2015, pp. 98 a 108.

GONZÁLEZ SERRANO, L.; LAGUNA SÁNCHEZ, P., «Comercio electrónico y empresa: panorama actual y perspectivas futuras», en Botana García, G.A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 65 a 108.

GOULD, M., «Rules in the virtual society», *International review of Law, computers & technology*, vol. 2, 1996, pp. 199 a 218.

GRAY, J., *False dawn: The delusions of global capitalism*, Nueva York, The New Press, 2000.

GRUPO DE TRABAJO DE COMUNICACIÓN Y DIVULGACIÓN, *DNI electrónico: guía de referencia básica*, Madrid, Comisión Técnica de Apoyo a la Implantación del DNI electrónico, 2014.

GUBERN GARRIGA-NOGUES, R., *El simio informatizado*, Milán, Fundesco, 1987.

GUERRERO CLAVIJO, R., «Novedades en materia de contratación mercantil introducidas por la Ley de Servicios de la Sociedad de la Información», *CEFLegal: revista práctica de derecho. Comentarios y casos prácticos*, vol. 47, 2004, pp. 3 a 28.

GUILLÉN CATALÁN, R., «La protección jurídica de los consumidores ante el envío de comunicaciones comerciales por vía electrónica», en Plaza Penadés, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, pp. 103 a 176.

GUILLIEN, R.; VINCENT, J., *Lexique de termes juridiques*, París, Dalloz, 1990.

HAGEL, J.; ARMSTRONG, A., *Net gain: expanding markets through virtual communities*, Brighton,

Harvard Business School Press, 1997.

HAINES, A., *Verbraucher schützende informationspflichten für websites: bedarfsgerechte angaben oder überregulierung?*, Münster, Universidad de Münster, 2008.

HARVARD UNIVERSITY, *Readiness for the networked world: a guide for developing countries*, Cambridge, Center for international development at Harvard University, 2000.

HEIDENREICH, M., «Die debatte um die wissensgesellschaft», en Böschen, S., Schulz-Schaeffer, I. (coords.) *Wissenschaft in der wissensgeseelschaft*, Opladen, Westdeutscher Verlag, 2003, pp. 1 a 25.

HEREDIA CERVANTES, I., «Consumidor pasivo y comercio electrónico internacional a través de páginas web», *Revista jurídica Universidad Autónoma de Madrid*, vol. 5, 2001, pp. 69 a 99.

HOLMES, O. W., *The common law*, Boston, Little Brown, 1923.

HORNING, R. A., «The enforceability of contracts negotiated in cyberspace», *International journal of Law and information technology*, vol. 2, 1997, pp. 109 a 157.

HORTALL I VALLVÉ, J.; ROCCATAGLIATA, F.; VALENTE, P., *La fiscalidad del comercio electrónico*, Valencia, Ciss, 2000.

HUERTA VIESCA, M. I., «La firma electrónica en la regulación española: valoración crítica», en Huerta Viesca, M.I., Rodríguez Ruiz de Villa, D. (coords.) *Los prestadores de servicios de certificación en la contratación Electrónica*, Cizur Menor, Aranzadi, 2001, pp. 21 a 47.

HUIDOBRO MOYA, J. M., «El modelo de negocio de las subastas electrónicas (e-Auctions)», *Bit*, vol. 164, 2007, pp. 60 a 63.

IBÁÑEZ MUÑOZ, J., *Poder y autoridad en las relaciones internacionales: el control del comercio electrónico en Internet*, Barcelona, Universitat Pompeu Fabra, 2004.

IHERING, R. V., *Geist des römischen rechts auf den verschiedenen stufen seiner entwicklung*, Leipzig, Breitkopf und Härtel, 1865.

ILLESCAS ORTIZ, R., *Derecho de la contratación electrónica*, Cizur Menor, Aranzadi, 2009.

ILLESCAS ORTIZ, R., «Entre Europa y la nada: a propósito del Anteproyecto de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico de 29 de septiembre de 2000», *Revista de la contratación electrónica*, vol. 11, 2000, pp. 3 a 33.

ILLESCAS ORTIZ, R., «La equivalencia funcional como principio elemental del Derecho del comercio electrónico», *Revista Derecho y tecnología*, vol. 1, 2000, pp. 9 a 23.

ILLESCAS ORTIZ, R., «La firma electrónica y el Real Decreto-ley 14/1999 de 17 de septiembre», *Derecho de los negocios*, vol. 109, 1999, pp. 1 a 14.

ILLESCAS ORTIZ, R., «La Ley 22/2007 sobre comercialización a distancia de servicios financieros destinados a los consumidores y la dogmática contractual electrónica», *Derecho de la contratación electrónica*, vol. 84, 2007, pp. 3 a 23.

ILLESCAS ORTIZ, R., «Oferta, perfección y prueba del contrato electrónico», *Estudios de Derecho judicial*, vol. 50, 2004, pp. 215 a 242.

ILLESCAS ORTIZ, R.; PERALES VISCASILLAS, P., *Derecho mercantil internacional. El Derecho uniforme*, Madrid, Centro de estudios Ramón Areces, 2003.

IRTI, N., *La edad de la descodificación*, Vallirana, Bosch, 1992.

JIMÉNEZ DE PARGA CABRERA, R., «El comercio electrónico ¿seguridad jurídica?», *Derecho de los negocios*, vol. 118 y 119, 2000, pp. 1 a 12.

JOLY-PASSANT, E., *L'écrit confronté aux nouvelles technologies*, París, Lgdj, 2006.

JOYANES AGUILAR, L., *Cibersociedad. Los retos sociales ante un nuevo mundo digital*, Madrid, McGraw-Hill, 1997.

JULIÀ BARCELÓ, R., *Comercio electrónico entre empresarios: la formación y prueba del contrato electrónico (EDI)*, Valencia, Tirant lo Blanch, 2000.

KALAKOTA, R.; WHINSTON, A. B., *Electronic commerce: A manager's guide*, Nueva York, Addison-Wesley, 1997.

KÜSTER, I.; HERNÁNDEZ, A., «From Web 2.0 to Web 3.0: antecedents and consequences of the attitude and use intention of social Networking in the semantic Web», *Universia Business Review*, vol. 37, 2013, pp. 104 a 119.

LAFUENTE SUÁREZ, M., «Análisis de la Ley 59/2003, de firma electrónica, tras dos años de vigencia: problemas no resueltos en torno a los certificados de firma electrónica», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 11, 2006, pp. 1 a 17.

LAFUENTE SUÁREZ, M., «El "nuevo" Reglamento UE 910/2014, relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior, tras un año desde su publicación en el DOUE», *Actualidad jurídica Aranzadi*, vol. 911, 2015, pp. 12 a 18.

LEINER, B. M.; CERF, V. G.; CLARK, D. D.; KAHN, R. E.; KLEINROCK, L.; LYNCH, D. C. Y OTROS, «A brief history of the Internet», *Internet society*, vol. 5, 1997, pp. 22 a 31.

LEMLEY, M. A.; LESSIG, L., *The end of end-to-end: preserving the architecture of the Internet in the broadband*, Los Ángeles, Ucla Law Review, 2000.

LEONE, C., «EU Regulation no. 910/2014 on electronic identification and trust services: an effort towards the elimination of barriers for electronic transactions and internal market consolidation», *Rivista italiana di Diritto pubblico comunitario*, vol. 3-4, 2015, pp. 1045 a 1060.

LEVITT, T., «Globalization of markets», *Harvard business review*, vol. 3, 1983, pp. 3 a 82.

LÉVY, P., *Qu'est-ce que le virtuel?*, París, La Découverte, 1998.

LINARES LÓPEZ, J.; ORTIZ CHAPARRO, F., *Autopistas inteligentes*, Madrid, Fundesco, 1996.

LISI, A.; GIACOPUZZI, L., *Guida al Codice dell'amministrazione digitale: con focues su archiviazione e fatturazione elettronica*, Matelica, Halley, 2006.

LOMASCOLO SZITTYAY, R., «Aspectos técnicos de la firma electrónica», en Pública, I.N. de A. (coord.) *Firma digital y Administraciones públicas*, Madrid, Instituto Nacional de Administración Pública, 2003, pp. 29 a 82.

LÓPEZ JIMÉNEZ, D.; MARTÍNEZ LÓPEZ, F. J., «La formación del contrato electrónico», *Revista de la contratación electrónica*, vol. 105, 2009, pp. 3 a 58.

LÓPEZ JIMÉNEZ, D.; MARTÍNEZ LÓPEZ, F. J., «Los códigos de conducta como solución frente a la falta de seguridad en materia de comercio electrónico», *Revista de ciencias económicas*, vol. 1, 2010, pp. 117 a 139.

LÓPEZ RICHART, J., «Difamación en la web 2.0 y responsabilidad civil de los prestadores de servicios de alojamiento», *Derecho privado y Constitución*, vol. 26, 2012, pp. 143 a 201.

LORENTE HOWELL, J. L., «Banca electrónica y Reglamento elDAS», *Actualidad jurídica Aranzadi*, vol. 927, 2017, pp. 1 y 2.

LORENZETTI, R., *Comercio electrónico: documento, firma digital, contratos, daños, defensa del consumidor*, Buenos Aires, Abeledo-Perrot, 2001.

LUNA HUERTAS, P.; MARTÍNEZ LÓPEZ, F. J., «Sociedad de la información y el conocimiento y nuevos paradigmas del Derecho: el caso de los códigos de conducta en el comercio electrónico», *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*, vol. 2, 2002, pp. 59 a 99.

MACHLUP, F., *The production and distribution of knowledge in the United States*, Princeton, Princeton University Press, 1962.

MACRÌ, I.; MACRÌ, U.; PONTEVOLPE, G., *Il nuovo Codice dell'amministrazione digitale: le tecnologie informatiche e le norme che ne disciplinanol'uso, aggiornate al D.Lgs. n. 235/2010*, Milanofiori Assago, Wolters Kluwer, 2011.

MADRID PARRA, A., «Aspectos jurídicos de la identificación en el comercio electrónico», en Illescas Ortiz, R., Ramos Herranz, I. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, pp. 185 a 247.

MADRID PARRA, A., «Contratación electrónica», en Iglesias Prada, J.L. (coord.) *Estudios jurídicos en homenaje al profesor Aurelio Menéndez*, Madrid, Civitas, 1996, pp. 2913 a 2958.

MADRID PARRA, A., «Contratación electrónica y protección de datos personales», *Revista de la contratación electrónica*, vol. 94, 2008, pp. 3 a 84.

MADRID PARRA, A., «Contratos electrónicos y contratos informáticos», *Revista de la contratación electrónica*, vol. 111, 2011, pp. 5 a 35.

MADRID PARRA, A., «Instrumentos de la CNUDMI/UNCITRAL sobre comercio electrónico (contratación, firma y comunicaciones comerciales)», en Plaza Penadés, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, pp. 299 a 408.

MADRID PARRA, A., «La identificación en el comercio electrónico», *Revista de la contratación electrónica*, vol. 15, 2001, pp. 3 a 60.

MADRID PARRA, A., «Seguridad en el comercio electrónico», en Orduña Moreno, F.J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, pp. 126 a 145.

MAESTRI, E., *Lex informatica: Diritto, persona e potere nell'età del cyberspazio*, Nápoles, Edizioni Scientifique Italiane, 2015.

MARÍN LÓPEZ, A., «Orden jurídico internacional y Constitución española», *Revista de Derecho político*, vol. 45, 1999, pp. 35 a 67.

MÁRQUEZ LOBILLO, P., *Empresarios y profesionales en la sociedad de la información*, Madrid, Edersa, 2004.

MÁRQUEZ LOBILLO, P., «Prestadores de servicios de intermediación: algunas especialidades de su estatuto jurídico», *Revista de la contratación electrónica*, vol. 88, 2007, pp. 3 a 31.

MARTÍN REYES, M. Á., «Los servicios de la sociedd de la información: ámbito coordinado y sujetos de los mismos», *Revista de la contratación electrónica*, vol. 41, 2003, pp. 3 a 26.

MARTÍNEZ NADAL, A., *Comentarios a la Ley 59/2003 de firma electrónica*, Cizur Menor, Aranzadi, 2004.

MARTÍNEZ NADAL, A., «Comentarios de urgencia al urgentemente aprobado Real Decreto-ley 14/1999 de 17 de septiembre, sobre firma electrónica», *La ley: revista jurídica española de doctrina, jurisprudencia y bibliografía*, vol. 6, 1999, pp. 1860 a 1871.

MARTÍNEZ NADAL, A., «Comercio electrónico», en Botana García, G.A., Ruiz Muñoz, M. (coords.) *Curso sobre protección jurídica de los consumidores*, Madrid, McGraw-Hill, 1999, pp. 247 a 273.

MARTÍNEZ NADAL, A., *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, Civitas, 2000.

MARTÍNEZ NADAL, A., «Firma electrónica», en Botana García, G.A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 159 a 200.

MARTÍNEZ NADAL, A., «Firma electrónica, certificados y entidades de certificación», *Revista*

*de la contratación electrónica*, vol. 68, 2006, pp. 41 a 64.

MARTÍNEZ NADAL, A., «Identificación y firma electrónica en el entorno digital», en Peguera Poch, M. (coord.) *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010, pp. 218 a 268.

MARTÍNEZ NADAL, A., *La Ley de firma electrónica*, Madrid, Civitas, 2000.

MARTÍNEZ NADAL, A., «La ley española de firma electrónica (Real Decreto Ley 14/1999)», en Illescas Ortiz, R., Ramos Herranz, I. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, pp. 77 a 116.

MARTÍNEZ NADAL, A., «La protección del consumidor en la Propuesta de Directiva sobre determinados aspectos del comercio electrónico», *Cuadernos de Derecho y comercio*, vol. 29, 1999, pp. 111 a 156.

MARTÍNEZ NADAL, A., «Problemática jurídica de los certificados de atributos en el comercio electrónico. En especial, su discordancia con el Registro Mercantil», en Orduña Moreno, F.J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, pp. 659 a 709.

MARTÍNEZ SÁNCHEZ, R.; GARCÍA BELTRÁN, A., «Breve historia de la informática», *División de informática industrial*, vol. 1, 2000, pp. 1 a 20.

MARTONI, M., *Firme elettroniche: profili informatico-giuridici*, Roma, Aracne, 2010.

MAS, F., *La conclusion des contrats du commerce électronique*, París, Lgdj, 2005.

MASUDA, Y., *The information society as post-industrial society*, New Brunswick, Transaction Publishers, 1980.

MCLUHAN, M., *The Gutenberg galaxy: the making of typographic man*, Toronto, University of Toronto Press, 1962.

MELIÁN ALZOLA, L., *La gestión de la calidad en el comercio electrónico desde la perspectiva del cliente*, Santa Cruz de Tenerife, Fundación Fyde-Caja Canarias, 2005.

MENÉNDEZ MATO, J. C.; GAYO SANTA CECILIA, M. E., *Derecho e informática: ética y legislación*, Vallirana, Bosch, 2014.

MERCADO IDOETA, C., *Banca en Internet: marketing y nuevas tecnologías*, Madrid, Dykinson, 1999.

MERCHÁN MURILLO, A., *Firma electrónica: funciones y problemática. Especial referencia al Reglamento [UE] nº 910/2014, relativo a la identificación electrónica por la que se deroga la Directiva 1999/93/CE de firma electrónica*, Cizur Menor, Aranzadi, 2016.

MIRANDA SERRANO, L. M.; PAGADOR LÓPEZ, J., «La formación y ejecución del contrato electrónico: aproximación a una realidad negocial emergente», *Estudios de consumo*, vol. 85, 2008, pp. 77 a 92.

MIRANDA SERRANO, L. M.; VELA TORRES, P. J.; PRÍES PICARDO, A., *La contratación mercantil. Disposiciones generales. Protección de los consumidores*, Madrid, Marcial Pons, 2006.

MOLINA MATEOS, J. M., «Libertad informática y criptología», *Informática y Derecho: revista iberoamericana de Derecho informático*, vol. 12, 1996, pp. 971 a 982.

MOLINÍ FERNÁNDEZ, F., «Ventajas, inconvenientes e impactos territoriales del comercio electrónico», *Investigaciones geográficas*, vol. 27, 2002, pp. 131 a 150.

MONCADA FLÓREZ, J. P., *La responsabilidad de los prestadores de servicios de intermediación en la sociedad de la información*, Granada, Universidad de Granada, 2009.

MONTERO AROCA, J., *La prueba en el proceso civil*, Madrid, Civitas, 2001.

MONTERO ELENA, M., «Incidencias del comercio electrónico en el Derecho comunitario», *Anuario de Derecho europeo*, vol. 1, 2001, pp. 133 a 147.

MORENO DELGADO, M.; SAN MARTÍN SEGURA, D., «La regulación de la firma electrónica modificaciones introducidas por el borrador de anteproyecto de Ley en relación al Real Decreto-ley 14/1999», *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja*, vol. 2002, pp. 1 a 19.

MORENO NAVARRETE, M. Á., *Contratos electrónicos*, Madrid, Marcial Pons, 1999.

MORENO NAVARRETE, M. Á., *Derecho-e: Derecho del comercio electrónico*, Madrid, Marcial Pons, 2002.

MUNAR BERNAT, P. A., «Protección de datos en el comercio electrónico», en Botana García, G.A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, Wolters

Kluwer, 2001, pp. 275 a 308.

MUÑOZ MACHADO, S., *La regulación de la Red: poder y Derecho en Internet*, Taurus, Barcelona, 2000.

NESPOR, S.; CESARIS, A. L., *Internet e la legge: la persona, la proprietà intellettuale, il commercio elettronico, gli aspetti penalistici*, Milán, Hoepli, 2001.

NORDHAUSEN, A., «Information requirements in e-commerce Directive and the proposed Directive on unfair commercial practices», en Janssen, A. (coord.) *Information rights and obligations: a challenge for party autonomy and transactional fairness,* Londres, Ashgate, 2004, pp. 93 a 114.

NORTON, J. J.; REED, C.; WALDEN, I., *Cross-border electronic banking: challenges and opportunities*, Londres, Lloyd's, 1995.

O'REILLY, T., *What is Web 2.0?: design patterns and business Models for the next generation of software*, Sebastopol, O'Reilly Media, 2005.

OLIVENCIA RUIZ, M., «De nuevo la Lección 1.ª. Sobre el concepto de la asignatura. Discurso leído en la solemne apertura del curso académico», 1999, Universidad de Sevilla.

ORDUÑA MORENO, F. J., *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003.

ORTEGA DÍAZ, J. F., *La firma y el contrato de certificación electrónicos*, Cizur Menor, Aranzadi, 2008.

ORTIZ NAVACERRADA, S., *La prueba de documentos en el proceso civil: estudio jurisprudencial*, Alcobendas, Actualidad, 1994.

PAGADOR LÓPEZ, J., *Condiciones generales y cláusulas contractuales predispuestas: la Ley de condiciones generales de la contratación de 1998*, Madrid, Marcial Pons, 1999.

PAMBOUKIS, C., «Droit international privé holistique: droit uniforme et droit international privé», *Recueil des cours*, vol. 330, 2007, pp. 417 a 428.

PANEBIANCO, M., *Introduzione al Diritto comunitario comparato: Diritto internazionale e Diritto dell'integrazione nell'Europa comunitaria e in America Latina*, Aix-en-Provence, Edisud, 1985.

PAREJO NAVAS, T., «Análisis de las figuras esenciales del régimen jurídico de la firma electrónica la ley 59/2003, de 19 de diciembre de firma electrónica», *Revista de la contratación electrónica*, vol. 70, 2006, pp. 3 a 32.

PARISI, F., *Il contratto concluso mediante computer*, Padua, Cedam, 1987.

PARRA VALCARCE, D., «De Internet 0 a Web 3.0: un reto epistemológico para la comunidad universitaria», *Anàlisi: quaderns de comunicaciò i cultura*, vol. 36, 2008, pp. 65 a 78.

PASCUZZI, G., *Il Diritto dell'era digitale*, Bolonia, Il Mulino, 2006.

PAZ LLOVERAS, E., *Cómo exportar, importar y hacer negocios a través de Internet*, Barcelona, Gestión, 2000.

PEDRERO ESTEBAN, A., «Internet: cuestiones de seguridad en la Red», en Flecha Andrés, J.R. (coord.) *Marketing y recursos humanos*, Salamanca, Universidad Pontificia de Salamanca e Instituto de Estudios Europeos y Derechos Humanos, 2001, pp. 53 a 78.

PEGUERA POCH, M., *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010.

PEGUERA POCH, M.; TARRÉS VIVES, M., «Marco jurídico de los servicios de la sociedad de la información y del comercio electrónico», en Peguera Poch, M. (coord.) *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010, pp. 318 a 389.

PEÑA LÓPEZ, I., «Fundamentos tecnológicos del Derecho de la sociedad de la información», en Peguera Poch, M. (coord.) *Principios de Derecho de la sociedad de la información*, Cizur Menor, Aranzadi, 2010, pp. 51 a 123.

PEÑA LÓPEZ, I.; BALAGUÉ PUXAN, F., *Acción comunitaria en la Red*, Barcelona, Graó, 2012.

PEÑA MARTÍNEZ, M. Á.; CABALLERO SANZ, F., «La política de competencia y el sector de las telecomunicaciones en la UE», *Información comercial española*, vol. 747, 1995, pp. 87 a 104.

PERALES VISCASILLAS, P., «Forma del contrato», en Botana García, G.A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, Wolters Kluwer, 2001, pp. 365 a 404.

PÉREZ BES, F., *El Derecho de Internet*, Barcelona, Atelier, 2016.

PÉREZ PEREIRA, M., *Firma electrónica: contratos y responsabilidad civil*, Cizur Menor, Aranzadi, 2009.

PIEDELIEVRE, A., *Les transformations du formalisme dans les obligations civiles*, París, Thése Française, 1959.

PLANT, R., *Ecommerce. Formulación de una estrategia*, Madrid, Prentice Hall, 2001.

PLAZA PENADÉS, J., «Breve comentario a la Ley 34/2002, de servicios de la sociedad de la información y comercio electrónico», *Alfa-Redi*, vol. 107, n.º 11 a 52, 2002.

PLAZA PENADÉS, J., *Derecho y Nuevas Tecnologías de la Información y la Comunicación*, Cizur Menor, Aranzadi, 2013.

PLAZA PENADÉS, J., «Eficacia de la firma electrónica en los Registros de la Propiedad y Mercantil», *Revista crítica de Derecho inmobiliario*, vol. 667, 2001, pp. 2005 a 2046.

PLAZA PENADÉS, J., «El marco jurídico de la contratación electrónica», en Plaza Penadés, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, pp. 177 a 230.

PLAZA PENADÉS, J., «La firma electrónica (regulación en España y en la Unión Europea)», en Plaza Penadés, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, pp. 409 a 478.

PLAZA PENADÉS, J., «La firma electrónica y su regulación en el Derecho español», en Orduña Moreno, F.J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, pp. 531 a 581.

PLAZA PENADÉS, J., «La firma electrónica y su regulación en la Directiva 1999/93, de la Unión Europea», en Orduña Moreno, F.J. (coord.) *Contratación y comercio electrónico*, Valencia, Tirant lo Blanch, 2003, pp. 489 a 529.

PLAZA PENADÉS, J., «La Ley de servicios de la sociedad de la información y comercio electrónico», en Plaza Penadés, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, pp. 43 a 102.

PLAZA PENADÉS, J., «La responsabilidad civil en Internet: su regulación en el Derecho comunitario y su previsible incorporación al Derecho español», *La ley: revista jurídica*

*española de doctrina, jurisprudencia y bibliografía*, vol. 3, 2001, pp. 2167 a 2186.

PLAZA PENADÉS, J., *Propiedad intelectual y sociedad de la información: Tratados OMPI, Directiva 2001/29/CE y responsabilidad civil en la Red*, Cizur Menor, Aranzadi, 2002.

PORAT, M. U., *The information economy*, Michigan, University of Michigan Library, 1977.

PRIETO SANCHÍS, L., «Observaciones sobre las antinomias y el criterio de ponderación», *Cuadernos de Derecho público*, vol. 11, 2000, pp. 9 a 30.

PUIG BRUTAU, J., *Fundamentos de Derecho civil*, Vallirana, Bosch, 1979.

RAIMONDO, F., «Firme "digitali", crittographia e validità del documento elettronico», *Il diritto dell'informazione e dell'informatica*, vol. 1, 1996, pp. 151 a 172.

RAMOS MÉNDEZ, F., *Enjuiciamiento civil*, Vallirana, Bosch, 1997.

RAPPA, M., «Business models on the Web», en AA.VV. (coord.) *Managing the digital Enterprise*, Carolina del Norte, North Carolina University, 2002, pp. 1 a 16.

RECODER DE CASSO, E., «Algunas observaciones en torno a contratos, electrónica y fe pública», en De Ros Cerezo, R.M., Cendoya Méndez de Vigo, J.M. (coords.) *Derecho de Internet : la contratación electrónica y firma digital*, Cizur Menor, Aranzadi, 2000, pp. 117 a 122.

REIDENBERG, J. R., «Lex informatica: the formulation of information policy rules through technology», *Texas Law review*, vol. 3, 1998, pp. 553 a 593.

REVUELTA DOMÍNGUEZ, F. I.; PÉREZ SÁNCHEZ, L., *Interactividad en los entornos de formación on-line*, Barcelona, Uoc, 2009.

RIBAGORDA GARNACHO, A., «Seguridad informática», en Illescas Ortiz, R., Ramos Herranz, I. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, pp. 3 a 36.

RIBAGORDA GARNACHO, A., «Sistema de certificación: la firma y el certificado digital», en Fernández Ordoñez, M., Cremades García, J., Illescas Ortiz, R. (coords.) *Régimen jurídico de Internet*, Las Rozas, Wolters Kluwer, 2001, pp. 1313 a 1338.

RICO CARRILLO, M., «El Reglamento europeo sobre identificación y servicios de confianza

electrónicos», *Revista general de Derecho europeo*, vol. 35, 2015, pp. 2 a 24.

RICO CARRILLO, M., «La forma en la contratación electrónica», *Derecho de los negocios*, vol. 172, 2005, pp. 15 a 22.

RODRÍGUEZ ADRADOS, A., *Firma electrónica y documento electrónico*, Madrid, Consejo General del Notariado, 2004.

RODRÍGUEZ ARDURA, I., *Marketing.com*, Madrid, Pirámide, 2000.

RODRÍGUEZ COHARD, J. C.; BERNAL JURADO, E., «Las regiones objetivo 1 españolas en la sociedad de la información: el comercio electrónico como elemento de desarrollo», *Revista de estudios regionales*, vol. 67, 2003, pp. 107 a 136.

RODRÍGUEZ DE LAS HERAS BALLEL, T., *El régimen jurídico de los mercados electrónicos cerrados (e-Marketplaces)*, Madrid, Marcial Pons, 2006.

RODRÍGUEZ HERNÁNDEZ, J., «Firma electrónica. Sus efectos jurídicos», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 6, 2004, pp. 41 a 53.

RODRÍGUEZ LÓPEZ, N., «La cadena de valor en Internet: análisis de su estructura y agentes participantes», *Revista de la contratación electrónica*, vol. 62, 2005, pp. 65 a 88.

RODRÍGUEZ LÓPEZ, N.; VÁZQUEZ ABAD, J.; MARTÍNEZ CARBALLO, M., «El comercio electrónico y la asimetría de la información: una aproximación desde los costes de transacción», *Revista galega de economía: Publicación Interdisciplinar da Facultade de Ciencias Económicas e Empresariais*, vol. 1, 2003, pp. 167 a 192.

ROJO GIL, F.; ALAMILLO DOMINGO, I., «Firma y sello electrónicos: el porqué y el cómo de la implantación del nuevo reglamento europeo», *Red seguridad: revista especializada en seguridad informática, protección de datos y comunicaciones*, vol. 74, 2016, pp. 28 y 29.

ROPPO, V., *Il contratto*, Bolonia, Il Mulino, 1977.

ROSELLO, C., *Commercio elettronico: la governance di Internet tra Diritto statuale, autodisciplina, soft Law e lex mercatoria*, Milán, Giuffrè, 2006.

ROSELLO, C.; FINOCCHIARO, G. D.; TOSI, E., *Commercio elettronico, documento informatico e firma digitale: la nuova disciplina*, Turín, Giappichelli, 2003.

ROVIRA FERRER, I., «El DNI electrónico: un análisis crítico y global», *Revista Aranzadi de Derecho y nuevas tecnologías*, vol. 26, 2011, pp. 47 a 53.

RUBIO TORRANO, E., «Firma electrónica», *Aranzadi civil*, vol. 13, 1999, pp. 1 a 14.

RUBIO VELÁZQUEZ, R.; MUÑOZ MUÑOZ, R.; RODRÍGUEZ SAU, C., *La firma electrónica: aspectos legales y técnicos*, Barcelona, Experiencia, 2004.

RUGGERI, L., «ADR y ODR y su taxonomía. La identificación de caracteres», *Revista de Internet, Derecho y Política*, vol. 10, 2010, pp. 32 a 41.

SÁBADA CHALEZQUER, C., «Interactividad y comunidades virtuales en el entorno de la world wide web», *Comunicación y sociedad*, vol. 1, 2000, pp. 139 a 166.

SALVADOR AYESTARÁN, I., «La firma digital: una tecnología para la intercomunicación en la sociedad-red», *Revista española de documentación científica*, vol. 1, 2001, pp. 51 a 69.

SÁNCHEZ COLL, A., «Del EDI al comercio electrónico», *El comercio en la SI*, vol. 813, 2004, pp. 43 a 54.

SÁNCHEZ DEL CASTILLO, V., «Los servicios de la sociedad de la información, la convergencia de las telecomunicaciones y los servicios de la sociedad de la información en la Ley 34/2002 sobre el comercio electrónico», *Revista de la contratación electrónica*, vol. 73, 2006, pp. 3 a 83.

SÁNCHEZ GONZÁLEZ, G., «El sector emprendedor de las TIC, el comercio electrónico y la colaboración con usuarios», *Economía industrial*, vol. 370, 2008, pp. 87 a 102.

SANCHÍS CRESPO, C., *La prueba de soportes informáticos*, Valencia, Tirant lo Blanch, 1999.

SANCHÍS CRESPO, C.; CHAVELI DONET, E. A., *La prueba por medios audiovisuales e instrumentos de archivo en la LEC 1/2000: doctrina, jurisprudencia y formularios*, Valencia, Tirant lo Blanch, 2002.

SANJURJO REBOLLO, B., *Lexnet abogados: notificaciones electrónicas y presentación de escritos y demandas*, Madrid, Dykinson, 2016.

SANJURJO REBOLLO, B., *Manual de Internet y redes sociales: una mirada legal al nuevo panorama de las comunicaciones en la Red, con especial referencia al periodismo digital, propiedad intelectual, protección*

*de datos, negocios audiovisuales, e-commerce, consumidores, marketing*, Madrid, Dykinson, 2015.

SANTAMARÍA DÍAZ, F.; ESCOBAR ESPINAR, M., «Estrategias empresariales ante el comercio electrónico», *Información comercial española*, vol. 813, 2004, pp. 187 a 196.

SANTORO PASSARELLI, F., *Dottrine generali del Diritto civile*, Nápoles, Jovene, 1986.

SARTOR, G., *L'informatica giuridica e le tecnologie dell'informazione: corso d'informatica giuridica*, Turín, Giappichelli, 2012.

SARTORI, L., *Il divario digitale: Internet e le nuove disuguaglianze social*, Bolonia, Il Mulino, 2006.

SCOTTI, L. B., *Contratos electrónicos: un estudio desde el Derecho internacional privado argentino*, Buenos Aires, Eudeba, 2012.

SCOTTI, L. B., *Gobernanza global: alternativas para la regulación jurídica del ciberespacio*, Buenos Aires, Fedye, 2015.

SCOTTI, L. B., «Los escenarios del Derecho internacional privado actual: globalización, integración y multiculturalidad», en Fernández Arroyo, D., Moreno Rodríguez, J.A. (coords.) *Derecho internacional privado y Derecho de la integración. Libro homenaje a Roberto Ruíz Díaz Labrano*, Asunción, Cedep, 2013, pp. 1 a 22.

SEGURA DE LASSALETA, R., «La seguridad de la contratación en Internet: la firma electrónica», *Revista general de Derecho*, vol. 670, 2000, pp. 8999 a 9012.

SENNINGER, S. F., «The information economy», *Montana Business Quarterly*, vol. 1, 2001, pp. 1 a 13.

SENTÍS MELENDO, S., *La prueba: los grandes temas del Derecho probatorio*, Buenos Aires, Ejea, 1979.

SEOANE BALADO, E., *La nueva era del comercio: el comercio electrónico. Las TIC al servicio de la gestión empresarial*, Vigo, Ideaspropias, 2005.

SERRA DOMÍNGUEZ, M., «La prueba documental», en Alonso-Cuevillas Sayrol, J. (coord.) *Instituciones del nuevo proceso civil. Comentarios sistemáticos a la Ley 1/2000*, Madrid, Dijusa, 2000, pp. 256 a 268.

SHAW, M.; BLANNING, R.; STRADER, T.; WHINSTON, A., *Handbook on Electronic Commerce*, Berlín, Springer, 2000.

SMITH, B., «The third industrial revolution: Law and policy for the Internet», *Collected courses of the hague academy of international Law*, vol. 282, 2000, pp. 1 a 45.

SOLDATI, N., «La stipulazione on-line dei contratti commerciali», en AA.VV. (coord.) *Studi di diritto dell'economia e dell'impresa in memoria di Antonio Cicognani*, Padua, Cedam, 2012, pp. 609 a 652.

SOLÉ MORO, M. L., *Comercio electrónico: un mercado en expansión*, Madrid, Escuela superior de gestión comercial, 2000.

SORIANO ATIENZA, F. J., «Comercio electrónico y grandes superficies», en Ramos Herranz, I., Illescas Ortiz, R. (coords.) *Derecho del comercio electrónico*, Las Rozas, La Ley, 2001, pp. 369 a 400.

SORIANO MALDONADO, S., «La firma electrónica en la UE y España: panorama del marco regulatorio general», *Economía industrial*, vol. 338, 2001, pp. 79 a 86.

SOTO, J.; PÉREZ, J.; FEIJÓO, C., «Veinticinco años de la sociedad de la información en España: evolución tecnológica, globalización y políticas públicas», *Economía industrial*, vol. 349, 2003, pp. 63 a 82.

STOLL, P. T.; GOLLER, B., *Electronic commerce and the Internet*, Berlín, German Yearbook of International Law, 1998.

TAPSCOTT, D.; WILLIAMS, A. D., *Wikinomics: how mass collaboration changes everything*, Londres, Atlantic Books, 2010.

TARDÍO PATO, J. A., «El principio de especialidad normativa (lex specialis) y sus aplicaciones jurisprudenciales», *Revista de Administración pública*, vol. 162, 2003, pp. 189 a 225.

TOSI, E., *Il contratto virtuale*, Milán, Giuffrè, 2005.

TOSI, E., «La conclusione dei contratti online», en Tosi, E. (coord.) *I problemi giuridici di Internet*, Milán, Giuffrè, 2003, pp. 9 a 37.

TOURAINE, A., *La société post-industrielle: naissance d'une société*, París, Denoël, 1969.

TREJO DELARBRE, R., *La nueva alfombra mágica: usos y mitos de Internet*, Madrid, Fundesco, 1996.

TROTTER HARDY, I., «The proper legal regime for 'cyberspace'», *University of Pittsburgh Law Review*, vol. 55, 1994, pp. 993 a 1055.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, *Building Confidence: electronic commerce and development*, Ginebra, 2000.

URÍA MENÉNDEZ, R., *Derecho mercantil*, Madrid, Marcial Pons, 1999.

VALERO TORRIJOS, J.; MARTÍNEZ GUTIÉRREZ, R., «Las bases jurídicas de la modernización tecnológica en las Administraciones públicas», en Plaza Penadés, J. (coord.) *Derecho y nuevas tecnologías de la información y la comunicación*, Cizur Menor, Aranzadi, 2013, pp. 479 a 544.

VAN DELLEN, M., «Anonymity on the Internet. What does the concept of anonymity mean?», *Electronic Law Review*, vol. 9, 2002, pp. 1 a 6.

VARGAS GÓMEZ-URRUTIA, M., «Protección internacional de los consumidores, contratos y comercio electrónico», en Botana García, G.A. (coord.) *Comercio electrónico y protección de los consumidores*, Las Rozas, La Ley, 2001, pp. 637 a 687.

VATTIER FUENZALIDA, C., «De nuevo sobre el régimen legal de la firma electrónica: estudio del Anteproyecto de 26 de junio de 2002», *Actualidad civil*, vol. 1, 2003, pp. 137 a 150.

VATTIER FUENZALIDA, C., «El régimen legal de la firma electrónica», *Actualidad civil*, vol. 1, 2000, pp. 411 a 419.

VATTIER FUENZALIDA, C., «Responsabilidad contractual y extracontractual en el comercio electrónico», *Anuario de Derecho civil*, vol. 1, 2002, pp. 67 a 90.

VÁZQUE GARCÍA, R. J., «Tecnología digital y formalización contractual», *Informática y Derecho: revista iberoamericana de Derecho informático*, vol. 33, 2000, pp. 95 a 116.

VÁZQUEZ GALLO, E.; BERROCAL COLMENAREJO, J. J., *Comercio electrónico: material para el análisis*, Madrid, Centro de publicaciones del Ministerio de Fomento, 2000.

VEGA CLEMENTE, V., «Comercio electrónico y reactivación económica», *Revista de estudios económicos y empresariales*, vol. 26, 2014, pp. 319 a 333.

VEGA VEGA, J. A., *Contratos electrónicos y protección de los consumidores*, Madrid, Reus, 2005.

VEGA VEGA, J. A., *Derecho mercantil electrónico*, Madrid, Reus, 2015.

VEGA VEGA, J. A., «El documento jurídico. Problemas de la electronificación», *Revista de estudios económicos y empresariales*, vol. 25, 2013, pp. 145 a 192.

VEGA VEGA, J. A., «La forma en el negocio jurídico electrónico», *Revista de estudios económicos y empresariales*, vol. 23, 2011, pp. 125 a 163.

VICENT CHULIÁ, F., *Introducción al Derecho mercantil*, Valencia, Tirant lo Blanch, 2004.

VILA SOBRINO, X. A., «Aspectos técnicos para el desarrollo de aplicaciones de comercio electrónico», en Tato Plaza, A., Albor Baltar, Á.F. (coords.) *Comercio electrónico en Internet*, Madrid, Marcial Pons, 2001, pp. 45 a 66.

VILLAR PALASÍ, J. L., *Derecho administrativo. Introducción y teoría de las normas*, Madrid, Universidad Complutense, 1968.

VILLAR PALASÍ, J. L., «Más sobre las antinomias», en AA.VV. (coord.) *Don Luis Jordana de Pozas: creador de ciencia administrativa*, Madrid, Universidad Complutense, 2000, pp. 51 a 72.

VILLAR URIBARRI, J. M., «El régimen jurídico de los prestadores de servicios de la sociedad de la información», en AA.VV. (coord.) *Derecho de Internet: la Ley de servicios de la sociedad de la información y de comercio electrónico*, Cizur Menor, Aranzadi, pp. 387 a 414.

XALABARDER PLANTADA, R., «La responsabilidad de los prestadores de servicios en Internet (ISP) por infracciones de propiedad intelectual cometidas por sus usuarios», *Revista de Internet, Derecho y Política*, vol. 2, 2006, pp. 1 a 15.

## ÍNDICE DE JURISPRUDENCIA

España. Tribunal Supremo (Sala de lo Civil, Sección 1ª). Sentencia núm. 293/1994, de 24 de marzo.

España. Tribunal Supremo (Sala de lo Civil, Sección 1ª). Sentencia núm. 673/1996, de 30 de julio.

España. Tribunal Supremo (Sala de lo Penal, Sección 2ª). Sentencia núm. 380/1997, de 25 de marzo.

España. Tribunal Supremo (Sala de lo Penal, Sección 2ª). Sentencia núm. 865/1997, de 13 de junio.

Estados Unidos. Tribunal Supremo norteamericano. Sentencia núm. 96/511, de 26 de junio de 1997.

España. Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 2ª). Sentencia de 3 de noviembre de 1997.

España. Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 7ª). Sentencia de 16 de enero de 1998.

España. Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 2ª). Sentencia de 29 de septiembre de 2000.

España. Tribunal Supremo (Sala de lo Contencioso-Administrativo, Sección 7ª). Sentencia de 28 de febrero de 2001.

España. Tribunal Constitucional (Sala 1ª). Sentencia núm. 80/2002, de 8 de abril de 2002.

España. Tribunal Supremo (Sala de lo Civil, Sección Única). Sentencia núm. 356/2003, de 3 de abril

España. Tribunal Supremo (Sala de lo Civil, Sección 1ª). Sentencia núm. 631/2005, de 20 de julio.

España. Audiencia Nacional (Sala de lo Contencioso-Administrativo, Sección 1ª). Sentencia de 17 de mayo de 2007.

Luxemburgo. Tribunal de Justicia de la Unión Europea (Sala Cuarta). Sentencia núm. C-298/07, de 16 de octubre de 2008.

España. Audiencia Provincial de León (Sala de lo Civil, Sección 1ª). Auto núm. 474/2009, de 8 de octubre de 2009.

España. Audiencia Provincial de Álava (Sala de lo Civil, Sección 1ª). Auto núm. 120/2010, de 15 de septiembre de 2010.

España. Juzgado de 1ª Instancia de Badalona (Sala de lo Civil, Sección 6ª). Sentencia núm. 106/2011, de 8 de junio.

Luxemburgo. Tribunal de Justicia de la Unión Europea (Sala Tercera). Sentencia núm. C-419/12, de 5 de julio.

# ANEXOS

## Anexo I. Cuadro de principales diferencias entre la Web 1.0 y la Web 2.0[893]

| **Web 1.0** | **Web 2.0** |
|---|---|
| Sólo lectura | Lectura/escritura/colaboración |
| La Web como plataforma de lectura | La Web como plataforma de publicación |
| Inteligencia individual | Inteligencia colectiva |
| Estática | Dinámica |
| Participación limitada | Colaborativa y participativa |
| Ediciones oficiales | Ediciones en constante revisión |
| Basadas en texto | Multimedia |
| Almacenamiento en disco duro | La Web como espacio de almacenamiento |
| Lectura | Conversación |

*Anexo I. Diferencias entre la Web 1.0 y la Web 2.0. Fuente: Peña López, I./Balagué Puxan, F.*

[893] La fuente de información con la que se ha elaborado este cuadro proviene de la obra de PEÑA LÓPEZ, I./BALAGUÉ PUXAN, F., *Acción comunitaria en la Red*, Barcelona, Graó, 2012, p. 28.

# Anexo II. Cuadro comparativo de la normativa en materia de SSI que rige en España: DCE y LSSICE

| Concepto | UE | | España | |
|---|---|---|---|---|
| | DCE | | LSSICE | |
| | Artículos | Modificaciones | Artículos | Modificaciones |
| Objeto | 1 | - | 1 | - |
| Ámbito de aplicación | | - | 2 a 5 | Se modifica el párrafo 1 del artículo 4 por el artículo 4.1 LMISI |
| Definiciones | 2 | - | Anexo | Se deroga el punto 6 de la letra a) del anexo por la D. D. 18 LGCA |
| Principio de aplicación de la Ley del de país origen | 3.1, 3.3 y anexo | - | 2 a 5 | Se modifica el párrafo 1 del artículo 4 por el artículo 4.1 LMISI |
| Principio de libre prestación de SSI | 3.2, 3.3, 3.4, 3.5, 3.6 y anexo | - | 7 a 8 | Se modifica el artículo 8 por el artículo 4.2 LMISI / Se reenumeran los apartados 2, 3, 4 y 5 del artículo 8 como 3, 4, 5 y 6 y se añade el apartado 2 y la letra e) al apartado 1 del artículo 8 por la D. F. 43.1 y 2 LES (BOE núm. 55, de 5 de marzo de 2011) |
| Principio de no autorización previa | 4 | - | 6 | - |
| Información general exigida | 5 | - | 10 | Se añade el apartado 3 al artículo 10 por la D. A. 8.1 LFE / Se modifica el apartado 1.b) y f) del artículo 10 por el artículo 4.4 LMISI / Se modifica el apartado 1.f) del artículo 10 por la D. F. 2.1 LGT |
| Régimen jurídico | - | - | 19 | - |
| Información exigida en comunicaciones comerciales | 6 | - | 20 | Se modifica el artículo 20 por el artículo 4.9 LMISI / Se añade el apartado 4 al artículo 20 por el artículo 4.1 RDTDMIEGCE (BOE núm. 78, de 31 de marzo de 2012) / Se modifican los apartados 1 y 3 del artículo 20 por la D. F. 2.3 LGT |
| Comunicación comercial no solicitada | 7 | - | 21 | Se modifica el artículo 21 por la D. F. 1.1 ALGT (BOE núm. 264, de 4 de noviembre de 2003) / Se añade un párrafo al apartado 2 del artículo 21 por el artículo 4.2 RDTDMIEGCE / Se modifica el apartado 2 del artículo 21 por la D. F. 2.4 LGT |
| Derechos de los destinatarios de las comunicaciones electrónicas | - | - | 22 | Se modifica el artículo 22 por la D. F. 1.2 ALGT / Se modifica por el artículo 4.3 RDTD-MIEGCE / Se modifica el artículo 22 por la D. F. 2.5 LGT |
| Comunicaciones comerciales por profesiones reguladas | 8 | - | - | - |

| Concepto | UE | | España | |
|---|---|---|---|---|
| | DCE | | LSSICE | |
| | Artículos | Modificaciones | Artículos | Modificaciones |
| Validez y eficacia de la contratación por vía electrónica | 9 | - | 23 | - |
| Prueba de los contratos celebrados por vía electrónica | - | - | 24 | Se modifica el apartado 1 del artículo 24 por el artículo 4.10 LMISI |
| Intervención de terceros de confianza | - | - | 25 | - |
| Ley aplicable | - | - | 26 | - |
| Obligaciones previas a la contratación | 10 | - | 27 | Se modifica la rúbrica y los apartados 1 y 2 del artículo 27 por el artículo 4.11 LMISI |
| Información posterior a la celebración de un contrato por vía electrónica | 11 | - | 28 | Se modifica la rúbrica y los apartados 1 y 2 del artículo 28 por el artículo 4.11 LMISI |
| Lugar de celebración del contrato electrónico | - | - | 29 | - |
| Responsabilidad de los PSSI | - | - | 13 | - |
| Deber de colaboración de los PSSIi | - | - | 11 | Se modifica el artículo 11 por el artículo 4.5 LMISI |
| Obligaciones de información sobre seguridad de los PSSIi | - | - | 12 bis | Se añade el artículo 12 bis por el artículo 4.6 LMISI |
| Responsabilidad PSSIi: mera transmisión | 12 | - | 14 | - |
| Responsabilidad PSSIi: memoria tampón | 13 | - | 15 | - |
| Responsabilidad PSSIi: alojamiento de datos | 14 | - | 16 | - |
| Responsabilidad PSSIi: facilitación de enlaces a contenidos o instrumentos de búsqueda | - | - | 17 | Se modifica el apartado 2 del artículo 17 por el artículo 4.7 LMISI |
| Inexistencia obligación general de supervisión de los PSSIi | 15 | - | - | - |
| Códigos de conducta | 16 | - | 18 | Se modifica el apartado 3 del artículo 18 por el artículo 4.8 LMISI / Se modifica el apartado 1 del artículo 18 por la D. F. 2.2 LGT |
| Acción de cesación | 18 | - | 30 | - |
| Legitimación activa en la acción de cesación | - | - | 31 | Se modifica el párrafo a) del artículo 31 por el artículo 4.4 RDTDMIEGCE |

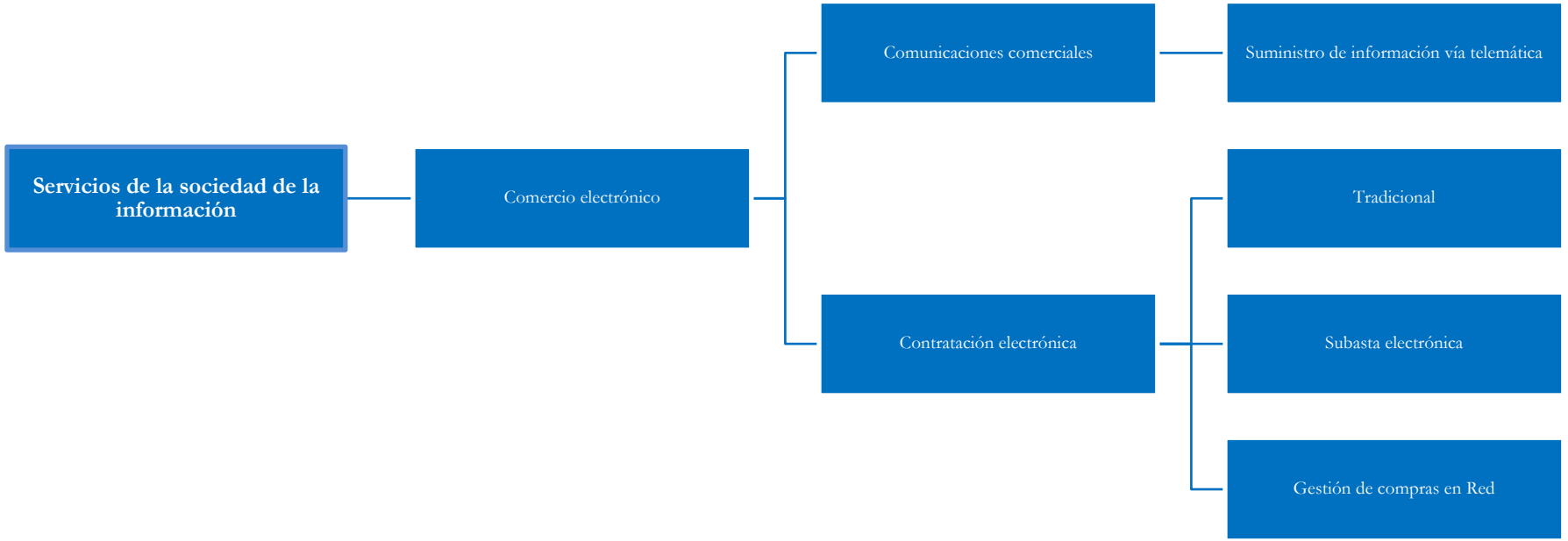
| Concepto | UE | | España | |
|---|---|---|---|---|
| | DCE | | LSSICE | |
| | Artículos | Modificaciones | Artículos | Modificaciones |
| Solución extrajudicial de litigios | 17 | - | 32 | - |
| Información a los PSSI y DSSI | - | - | 33 | Se modifica el artículo 33 por el artículo 4.12 LMISI |
| Comunicación de resoluciones relevantes | - | - | 34 | - |
| Supervisión y control | 19 | - | 35 | Se modifican los apartados 1 y 2 del artículo 35 por el artículo 4.13 LMISI / Se modifica el apartado 1 del artículo 35 por la D. F. 2.6 LGT |
| Deber de colaboración de los PSSI | 19 | - | 36 | - |
| Responsables | - | - | 37 | Se modifica el artículo 37 por la D. F. 2.7 LGT |
| Infracciones | - | - | 38 | Se modifican los apartados 3.b) y 4.d) del artículo 38 por la D. F. 1.3 y 4 ALGT / Se modifican los apartados 2, 3 y 4 del artículo 38 por la D. A. 8.2 LFE / Se derogan los apartados 2.c) y d) y 3.a) del artículo 38 por la D. D. Única.1 LCDRCE-RPC (BOE núm. 251, de 19 de octubre de 2007) / Se deja sin contenido el apartado 2.a) y se modifica el apartado 4.a), ambos del artículo 38, por el artículo 4.14 y 15 LMISI / Se modifican los apartados 3.c), 3.i) y 4.g) del artículo 38 por la D. F. 2.8 a 10 LGT |
| Sanciones | 20 | - | 39 | Redactado el apartado 2, párrafo 2, del artículo 39 conforme a la corrección de errores publicada en BOE núm. 187, de 6 de agosto de 2002 |
| Moderación de sanciones | - | - | 39 bis | Se añade el artículo 39 bis por la D. F. 2.11 LGT |
| Graduación de la cuantía de las sanciones | - | - | 40 | Se modifica el artículo 40 por la D. F. 2.12 LGT |
| Medidas de carácter provisional | - | - | 41 | - |
| Multa coercitiva | - | - | 42 | - |
| Competencia sancionadora | - | - | 43 | Se modifica el apartado 1 del artículo 43 por la D. F. 1.5 ALGT / Se modifican los apartados 1, párrafo segundo, y 2, ambos del artículo 43, por la D. A. 8.3 y 4 LFE/ Se modifica el artículo 43 por el artículo 4.16 LMISI / Se modifica por la D. F. 2.13 LGT |
| Concurrencia de infracciones y sanciones | - | - | 44 | - |
| Prescripción | - | - | 45 | - |

| Concepto | UE | | España | |
|---|---|---|---|---|
| | DCE | | LSSICE | |
| | Artículos | Modificaciones | Artículos | Modificaciones |
| Reexamen | 21 | - | - | - |
| Transposición | 22 | - | - | - |
| Destinatarios de la norma | 24 | - | - | - |
| Significado de los términos empleados por la Ley | - | - | D. A. 1ª | - |
| Medicamentos y productos sanitarios | - | - | D. A. 2ª | - |
| Sistema Arbitral de Consumo | - | - | D. A. 3ª | Se modifica la D. A. 3ª por el artículo 4.17 LMISI |
| Modificación de los CC y CCom | - | - | D. A. 4ª | - |
| Accesibilidad para las personas con discapacidad y de edad avanzada a la información proporcionada por medios electrónicos | - | - | D. A. 5ª | Se modifica el apartado 1 y se añaden los apartados 3, 4 y 5, todo de la D. A. 5ª, por el artículo 4.18, 19 y 20 LMISI / Se añade el apartado 6 de la D. A. 5ª por el artículo 16 LANCIDPD (BOE núm. 184, de 2 de agosto de 2011) |
| Sistema de asignación de nombres de dominio bajo el ".es" | - | - | D. A. 6ª | Se añade el apartado cinco bis de la D. A. 6ª por la D. F. 2.14 LGT |
| Fomento de la sociedad de la información | - | - | D. A. 7ª | Se añade la D. A. 7ª por la D. F. 1.6 ALGT. Redactado conforme a la corrección de errores publicada en BOE núm. 68, de 19 de marzo de 2004 |
| Colaboración de los registros de nombres de dominio establecidos en España en la lucha contra actividades ilícitas | - | - | D. A. 8ª | Se añade la D. A. 8ª por la D. F. 2.15 LGT |
| Gestión de incidentes de ciberseguridad que afecten a la red de Internet | - | - | D. A. 9ª | Se añade la D. A. 9ª por la D. F. 2.16 LGT |
| Anotación en los correspondientes registros públicos de los nombres de dominio otorgados antes de la entrada en vigor de la Ley | - | - | D. T. Única | - |
| Modificación del artículo 37 AALGT (BOE núm. 99, de 25 de abril de 1998) | - | - | D. F. 1ª | Esta D. F. 1ª entra en vigor el 13 de julio de 2002, según la D. F. 9ª |
| Modificación de la D. A. 6ª AALGT | - | - | D. F. 2ª | Esta D. F. 2ª entra en vigor el 13 de julio de 2002, según la D. F. 9ª |

| Concepto | UE | | España | |
|---|---|---|---|---|
| | DCE | | LSSICE | |
| | Artículos | Modificaciones | Artículos | Modificaciones |
| Adición de una nueva D. T. AALGT | - | - | D. F. 3ª | Esta D. F. 3ª entra en vigor el 13 de julio de 2002, según la D. F. 9ª |
| Modificación de la D. D. Única AALGT | - | - | D. F. 4ª | Esta D. F. 4ª entra en vigor el 13 de julio de 2002, según la D. F. 9ª |
| Adecuación de la regulación reglamentaria sobre contratación telefónica o electrónica con condiciones generales de esta Ley | - | - | D. F. 5ª | - |
| Fundamento constitucional | - | - | D. F. 6ª | - |
| Habilitación del Gobierno | - | - | D. F. 7ª | - |
| Distintivo de adhesión a códigos de conducta que incorporen determinadas garantías | - | - | D. F. 8ª | - |
| Entrada en vigor | 23 | - | D. F. 9ª | - |

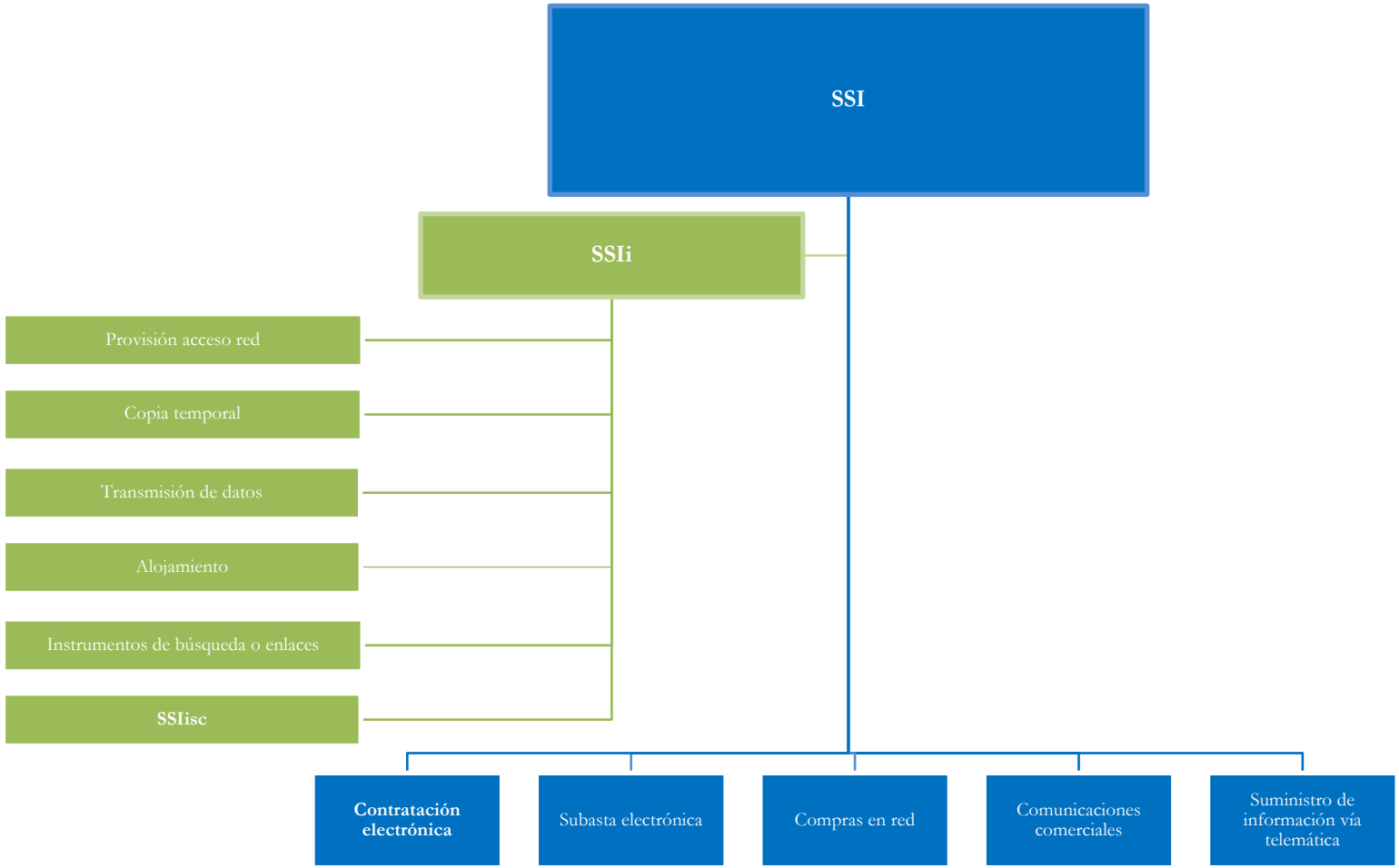
*Anexo II. Cuadro comparativo de la normativa en materia de SSI que rige en España: DCE y LSSICE. Fuente: elaboración propia*

# Anexo III. Servicios de la sociedad de la información integrados en la LSSICE y agrupados por categorías



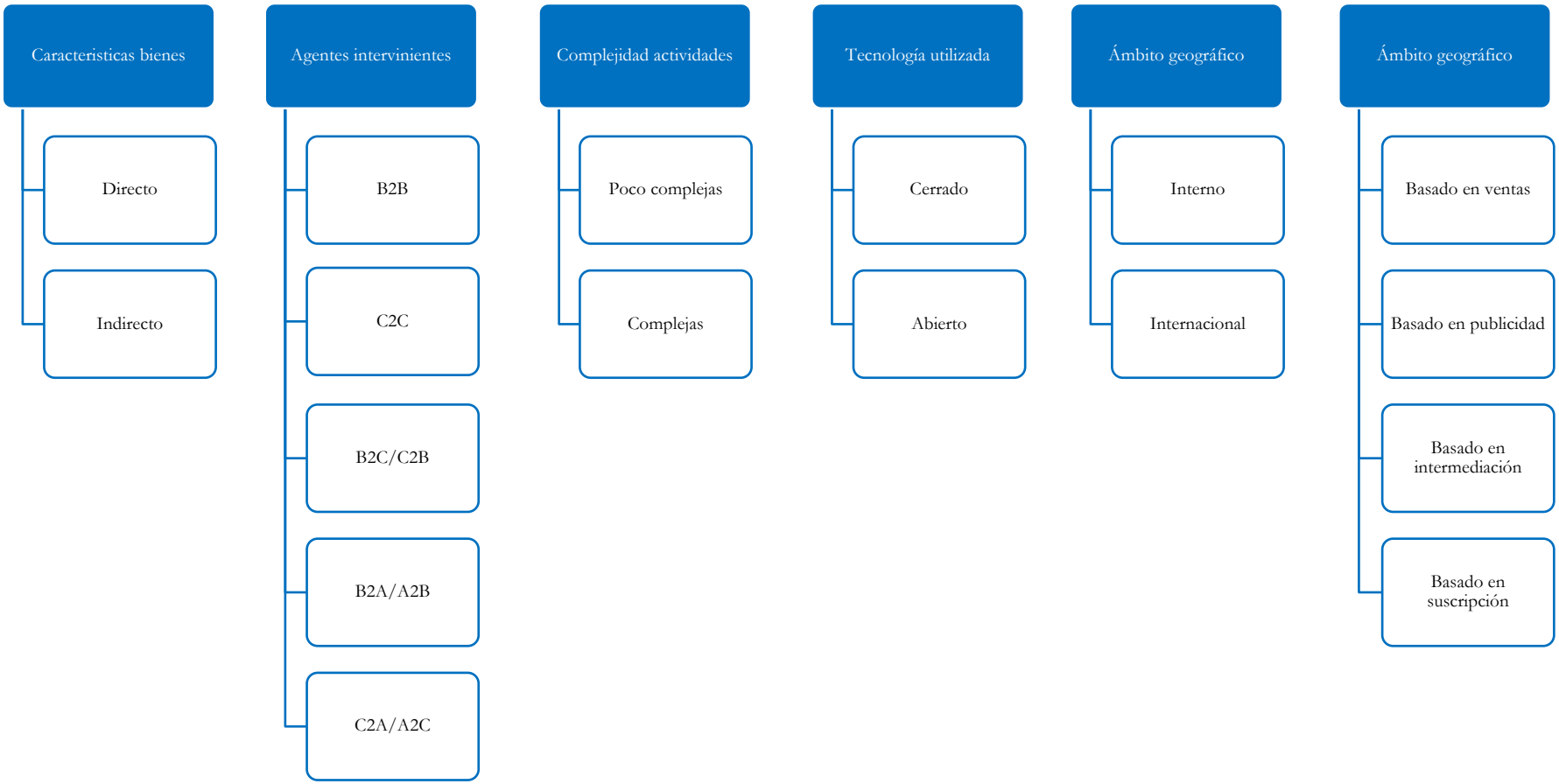

*Anexo III. Servicios de la sociedad de la información integrados en la LSSICE y agrupados por categorías. Fuente: elaboración propia.*

# Anexo IV. Servicios de la sociedad de la información



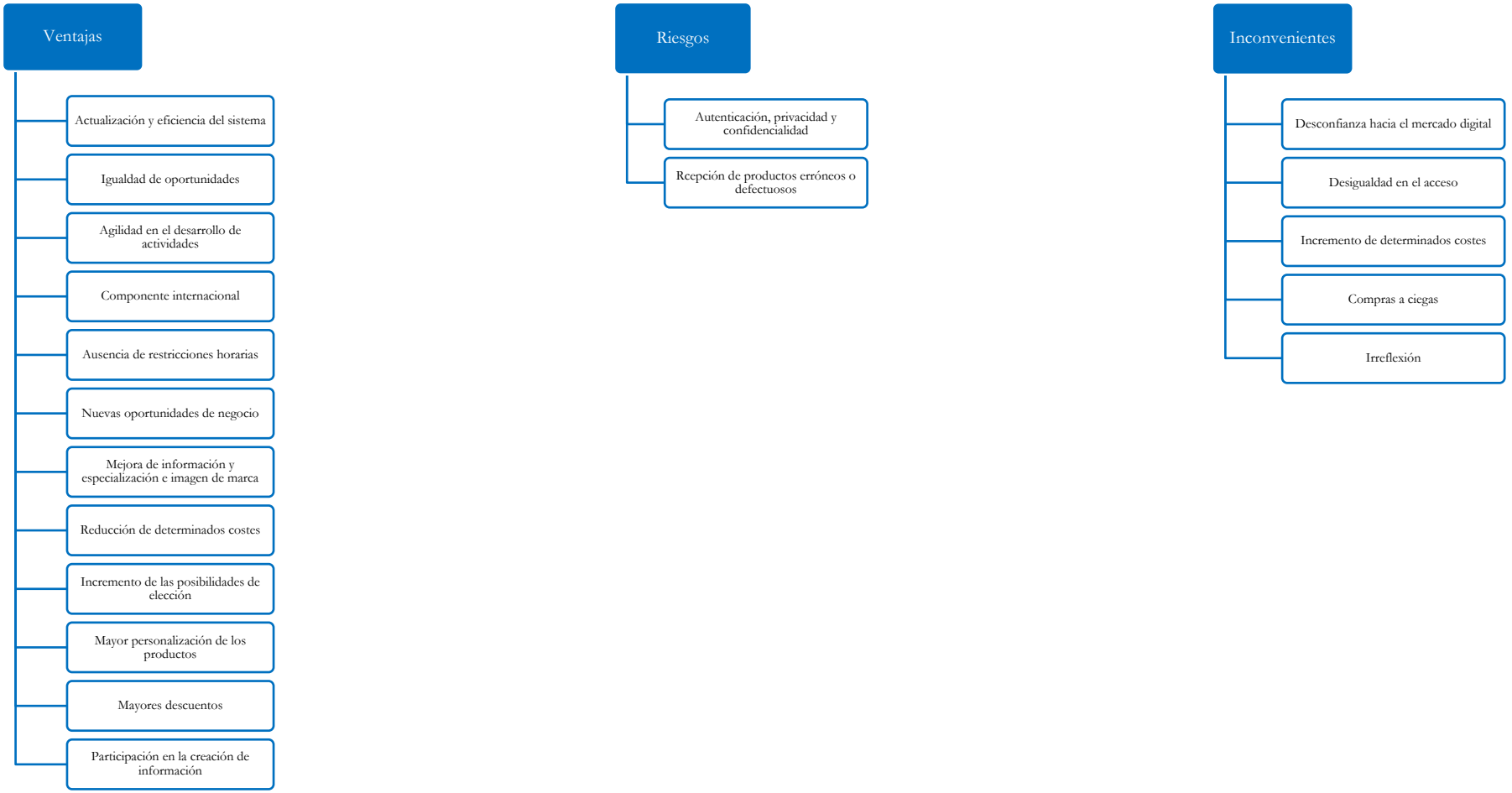

*Anexo IV. Servicios de la sociedad de la información. Fuente: elaboración propia.*

# Anexo V. Posibles clasificaciones de comercio electrónico



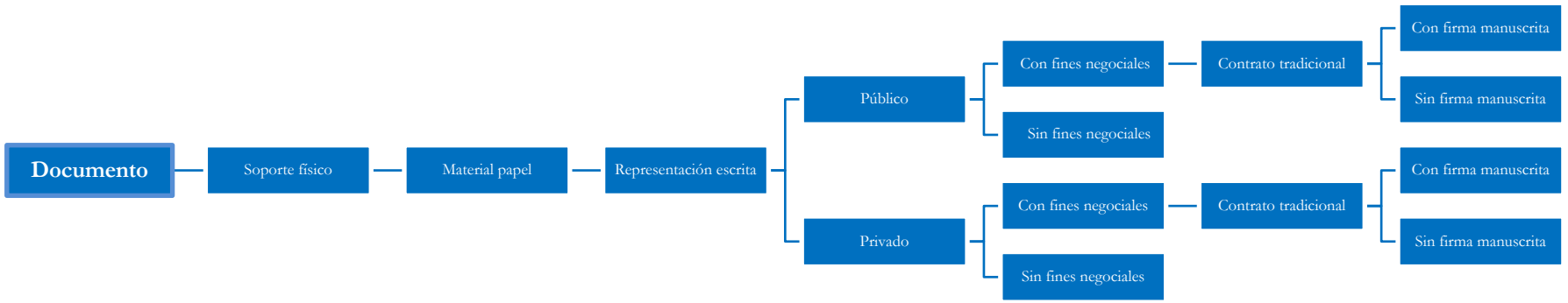

*Anexo V. Posibles clasificaciones de comercio electrónico. Fuente: elaboración propia.*

# Anexo VI. Ventajas, riesgos e inconvenientes del comercio electrónico



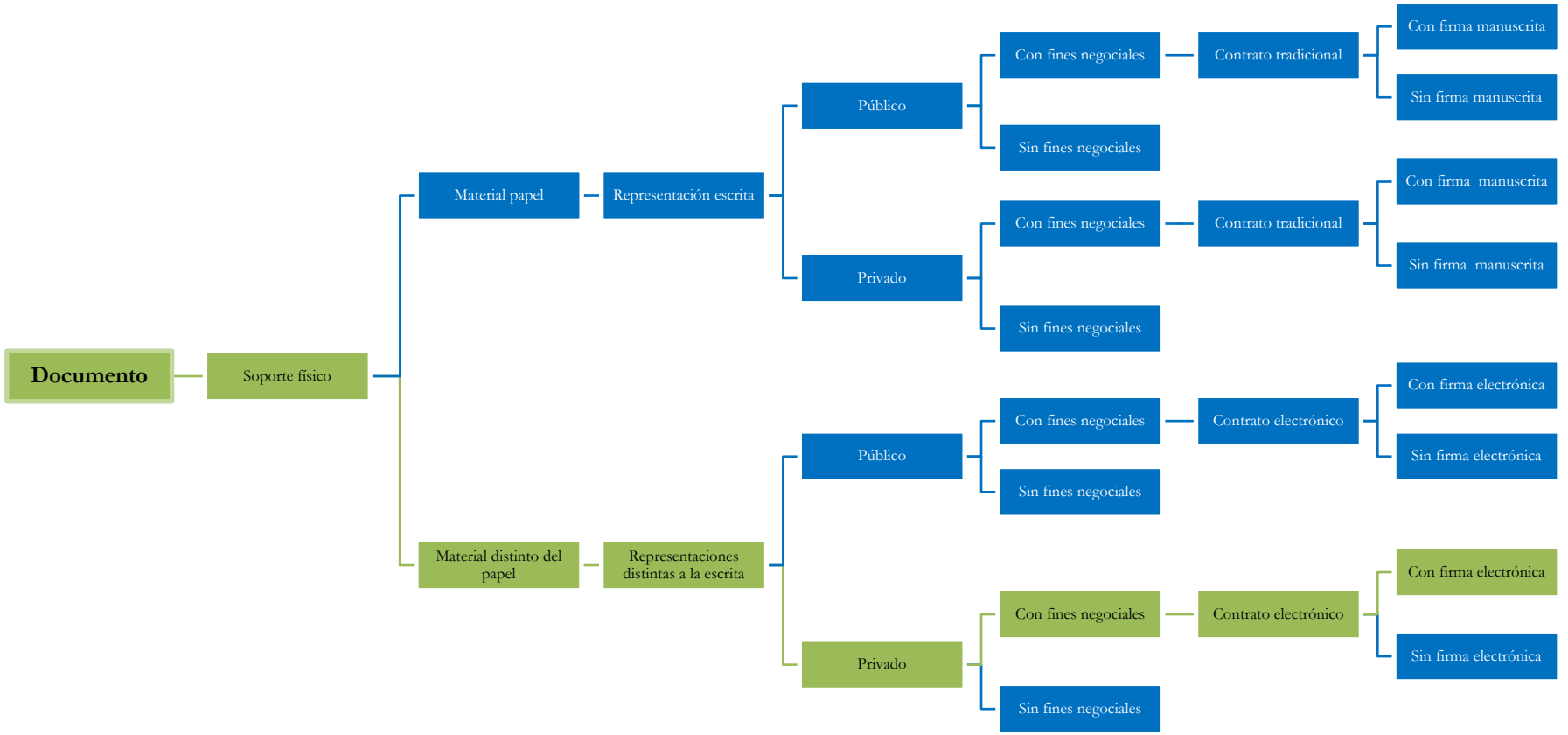

*Anexo VI. Ventajas, riesgos e inconvenientes del comercio electrónico. Fuente: elaboración propia.*

# Anexo VII. Esquema de la teoría estricta, del escrito, restringida o latina



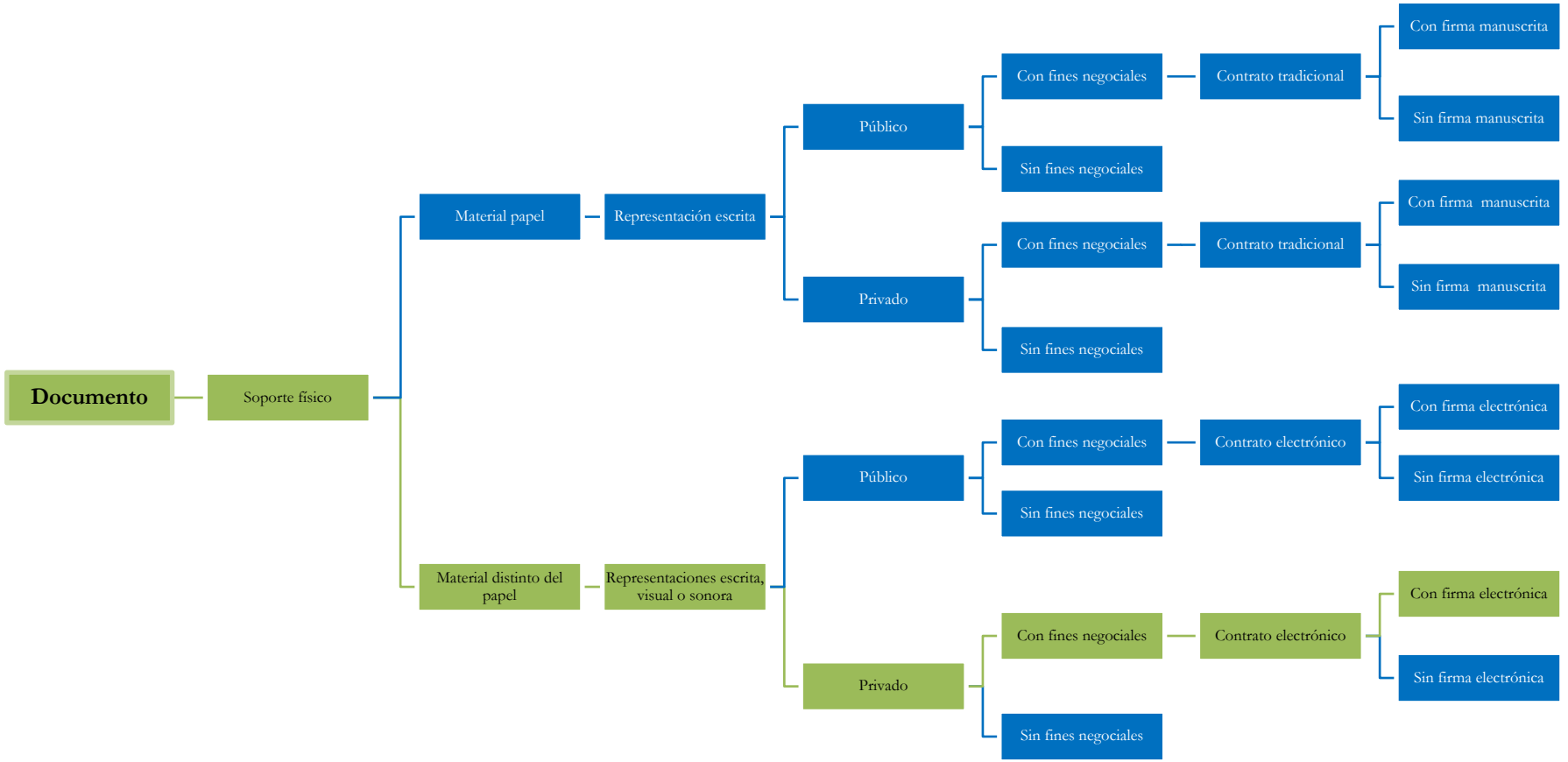

*Anexo VII. Esquema de la teoría estricta, del escrito, restringida o latina, desarrollada desde una perspectiva negocial. Fuente: elaboración propia.*

## Anexo VIII. Esquema de la teoría de la representación o germánica



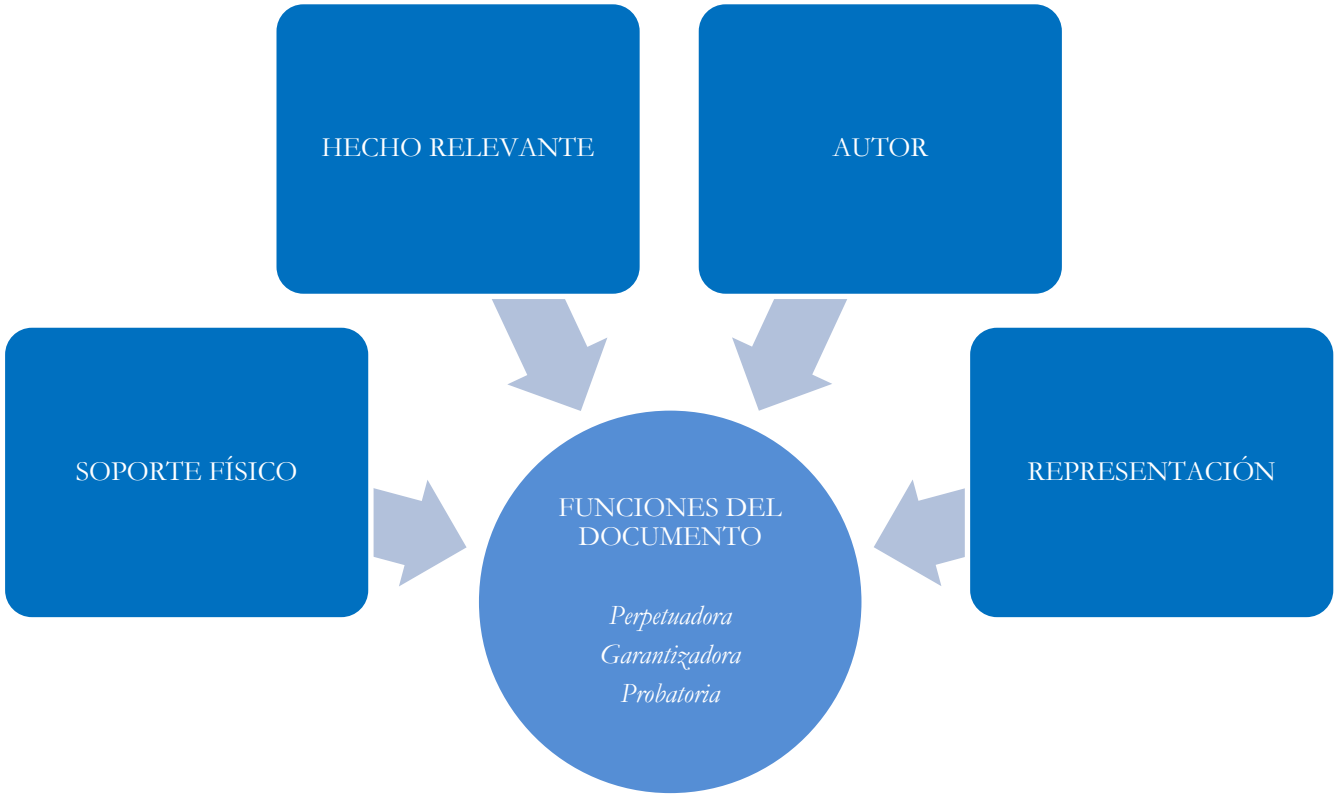

*Anexo VIII. Esquema de la teoría de la representación o germánica, desarrollada desde una perspectiva negocial (en verde aparece la línea argumental seguida en el presente estudio). Fuente: elaboración propia.*

# Anexo IX. Esquema de la teoría del documento como fin



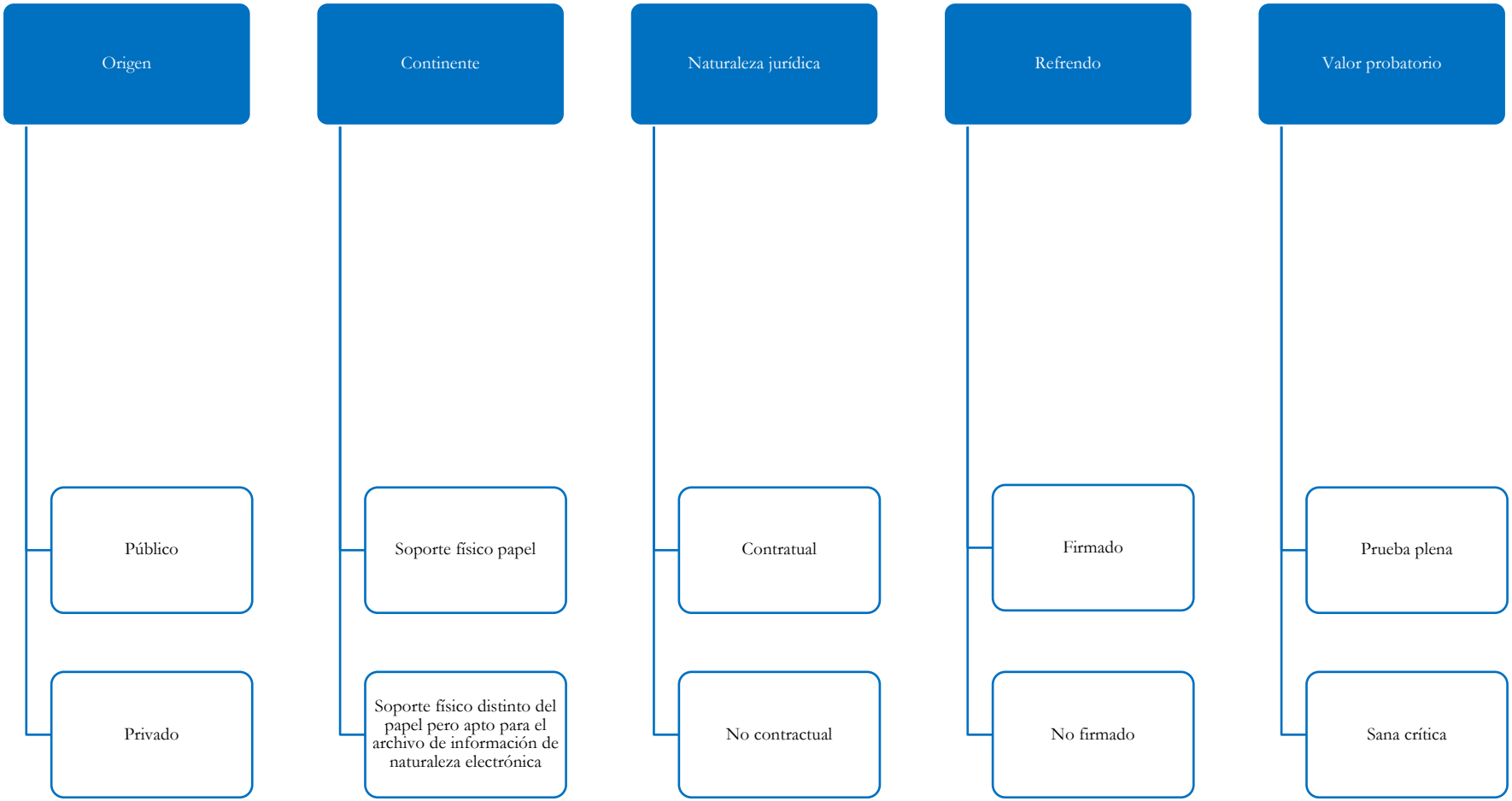

*Anexo IX. Esquema de la teoría del documento como fin, desarrollada desde una perspectiva negocial (en verde aparece la línea argumental seguida en el presente estudio). Fuente: elaboración propia.*

Anexo X. Elementos esenciales del documento



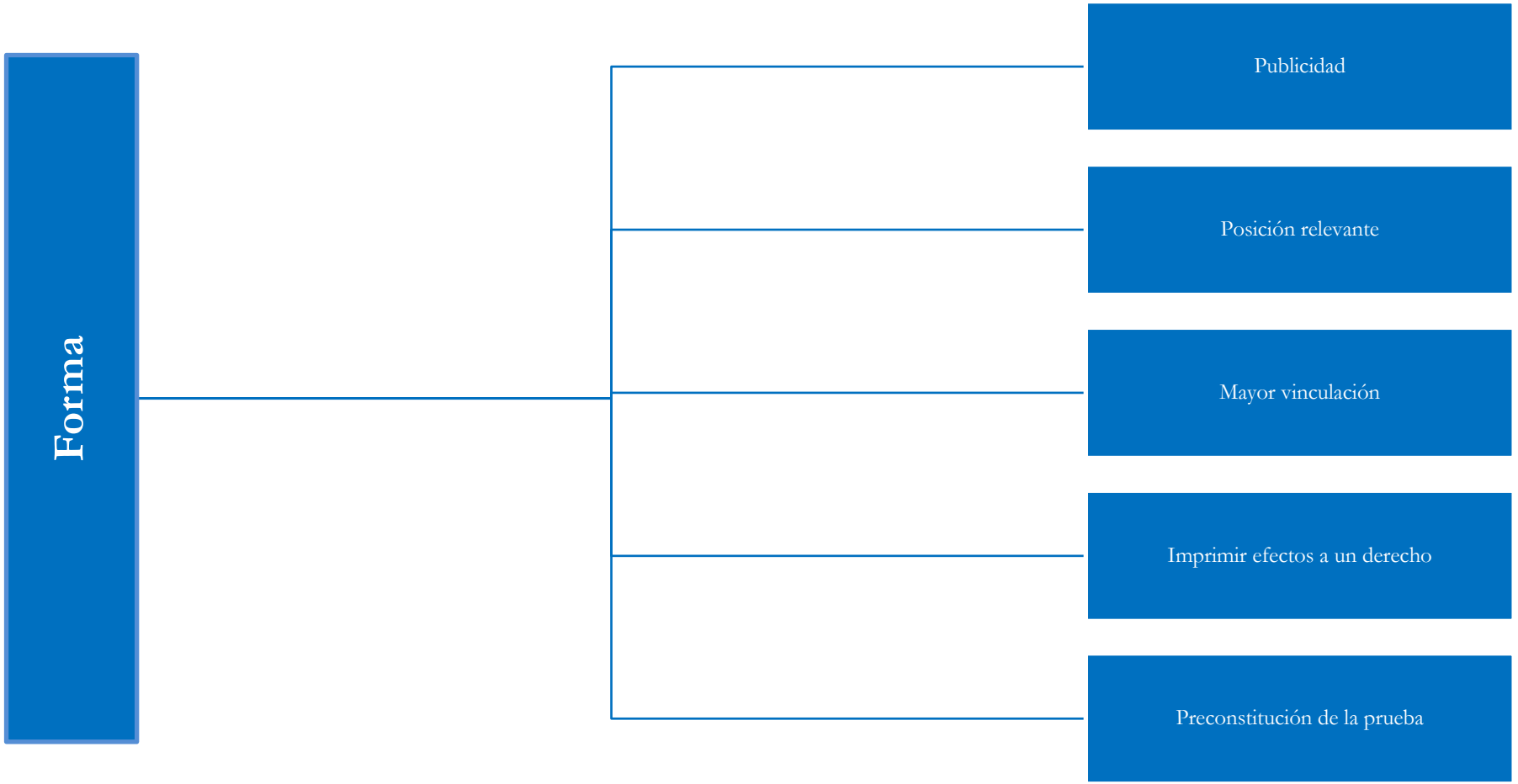

*Anexo X. Elementos esenciales del documento. Fuente: elaboración propia*

# Anexo XI. Posibles clasificaciones del documento



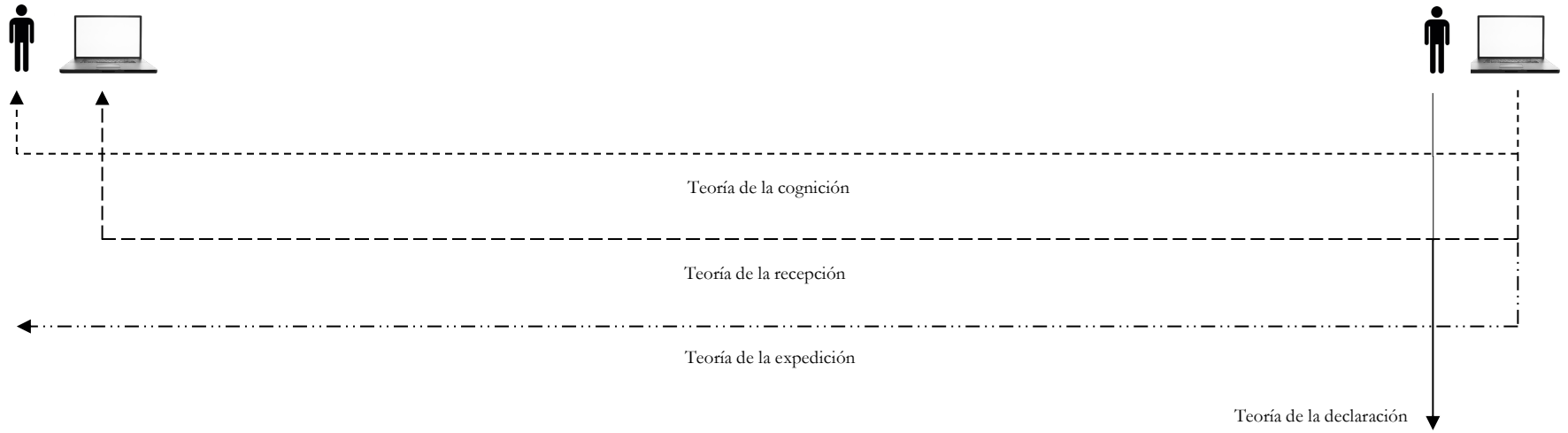

*Anexo XI. Posibles clasificaciones del documento. Fuente: elaboración propia.*

Anexo XII. Fines perseguidos con la forma en los contratos




*Anexo XII. Fines perseguidos con la forma en los contratos. Fuente: elaboración propia*

# Anexo XIII. Teorías en torno al momento de determinación de los contratos a distancia




*Anexo XIII. Teorías en torno al momento de determinación de los contratos a distancia. Fuente: elaboración propia*

# Anexo XIV. La Directiva sobre firma electrónica y su transposición al ordenamiento jurídico interno, español e italiano

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| Ámbito de aplicación/Objeto | 1 | 1 (1) | - | 1 (24) | - | 1 (49) | - | 2 (53) | Se modifica el apartado 5 del artículo 2 por el artículo 2 DLCAD / Se sustituye el apartado 2 del artículo 2 por la letra a) del apartado primero del artículo 2 PDLMICAD, siendo necesario acudir también al respecto al apartado 20 del artículo 57 PDLMICAD / Se deroga el apartado 2 bis del artículo 2 por la letra a) del apartado 1 del artículo 2 PDLMICAD / Se sustituye el apartado 3 del artículo 2 por la letra c) del apartado primero del artículo 2 PDLMICAD / Se modifica el apartado 6 del artículo 2 por la letra d) del apartado primero del artículo 2 PDLMICAD, siendo necesario acudir también al apartado primero del artículo 57 PDLMICAD, al DPCMMCAD (Gazzetta Ufficiale num. 69, 25 marzo 2011) y al DPCMCAD (Gazzetta Ufficiale num. 77, 4 aprile 2011) |
| | | | | 2.1, 2.3, 2.4 y 2.5 | - | | | | |
| Definiciones | 2.1) | 2.a) (2) | - | 3.1 (25) | - | 2.1.a) (50) | - | 1.q) | Se modifica el apartado q) del artículo 1 por el artículo 1 DLCAD y por la letra e) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.q bis) | Se incorpora este artículo por la letra e) del apartado primero del artículo 1 PDLMICAD |
| | 2.2) | 2.b) (3) | - | 3.2 (26) | Se modifica el apartado 2 del artículo 3 por la D. F. 4.1 LMSO (BOE núm. 180, de 29 de julio de 2015) | 2.1.g) | - | - | - |
| | 2.3) | 2.c) (4) | - | 6.2 (27) | Se modifica el apartado 2 del artículo 6 por la D. F. 4.2 LMSO | - | - | 1.aa) | - |
| | 2.4) | 2.d) | - | 24.1 | - | - | - | - | - |
| | 2.5) | 2.e) | - | 24.2 (28) | - | - | - | - | - |
| | 2.6) | 2.f) | - | 24.3, *ab initio*, y 28.1 | - | 2.1.f) | - | - | - |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| | 2.7) | 2.g) | - | 25.1 | - | - | - | - | - |
| | 2.8) | 2.h) | - | 25.2 | - | - | - | - | - |
| | 2.9) | 2.i) (5) | - | 6.1 | - | 2.1.d) | - | 1.e) | Se modifica el apartado e) del artículo 1 por el artículo 1 DLCAD |
| | 2.10) | 2.j) | - | 11.1 y 11.2 | - | 2.1.e) (51) | - | 1.f) | - |
| | 2.11) | 2.k) (6) | - | 2.2 (29) | - | 2.1.b) | - | 1.g) | - |
| | 2.12) | 2.l) | - | - | - | - | - | - | - |
| | 2.13) | 2.ll) (7) | - | - | - | 2.1.h) | - | - | - |
| | - | - | - | - | - | - | . | 1.a) | - |
| | - | - | - | - | - | - | . | 1.b) | Se modifica el apartado a) del artículo 1 por el artículo 1 DLCAD, después sustituido por la letra a) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | . | 1.d) | - |
| | . | . | - | . | . | . | . | 1.h) | - |
| | - | - | - | - | - | - | - | 1.i) | Se modifica el apartado i) del artículo 1 por la letra c) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.i bis) | Letra incorporada por la letra c) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.i ter) | Letra incorporada por la letra c) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.i quater) | Letra incorporada por la letra c) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.i quin-quies) | Letra incorporada por la letra c) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.l) | - |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| | - | - | - | - | - | - | - | 1.m) | - |
| | - | - | - | - | - | - | - | 1.n) | Se modifica el apartado n) del artículo 1 por el apartado segundo del artículo 9 DLUM |
| | - | - | - | - | - | - | - | 1.n bis) | Letra incorportada por el apartado 2 del artículo 9 DLUM |
| | - | - | - | - | - | - | - | 1.o) | - |
| | - | - | - | - | - | - | - | 1.s) | Se modifica el apartado s) del artículo 1 por la letra g) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.t) | Se modifica el apartado r) del artículo 1 por el artículo 1 DLCAD, después sustituido por la letra f) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.u) | Se modifica el apartado u) del artículo 1 por la letra h) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.u bis) | Letra incorporada por la letra h) del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.u ter) | Letra incorporada por la letra h) del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.v) | Se modifica el apartado v) del artículo 1 por la letra i) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.v bis) | Letra incorporada por la letra i) del apartado primero del artículo 1 PDLMICAD |
| | - | - | - | - | - | - | - | 1.z) | Véase también el artículo 48 DLDU (Gazzetta Ufficiale num. 147, 25 giugno 2008) |
| | - | - | - | - | - | - | - | 1.bb) | - |
| Acceso al mercado | 3.1 | 4.1 (8) | - | 5 (30) | - | 3 | - | 26 | Se modifica el apartado primero del artículo 26 por el apartado primero del artículo 18 PDLMICAD |
| | 3.6 | - | - | - | | - | - | - | - |
| | 3.7 | 5 | - | 3.11 y 4 (31) | - | 9 y 12 | - | 22 y 34 | Se modifica el artículo 22 por el artículo 10 DLCAD, después sustituido por el apartado primero del artículo 15 PDLMICAD, siendo necesario acudir también a estos efectos al apartado séptimo del artículo 57 PDLMICAD / Se modifica la letra a) del apartado primero |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| | | | | | | | | | del artículo 34 por el artículo 15 DLCAD / Se modifica el apartado segundo del artículo 34 por el artículo 15 DLCAD |
| Principios del mercado interior | 4 | 1.1, *in fine*, y 4.1, *in fine* (9) | - | 5 y 2 (32) | - | - | - | - | - |
| Efecto jurídico de la firma electrónica | 5 | 3 (10) | - | 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9 y 3.10 (33) | Se modifican los apartados 5 y 8 del artículo 3 por los artículos 5.1 y 5.2 LMISI / Se modifica el apartado 2 del artículo 3 por la D. F. 4.1 LMSO / Se añade el apartado 11 del artículo 3, con efectos de 2 de octubre de 2016, por la D. F. 2 LPACAP | 6.1, 6.2, 6.3, 6.4, 9.1 y 11.1 | El artículo 6 DLDFE sustituye al artículo 10 DPRDA. El artículo 6 DLDFE introduce un apartado 6 sin equivalencia en la DFE ni en la LFE. El artículo 9 DLDFE sustituye al artículo 38.2 DPRDA | 1.p), 1.p bis), 1.r), 20, 21.1, 21.2, 21.2 bis, 23, 23 bis, 23 ter, 23 quater, 24 y 25 (54) | Se modifica el apartado p) del artículo 1 por la letra d) del apartado primero del artículo 1 PDLMICAD / Se incorpora el artículo 1.p bis) por la letra d) del apartado primero del artículo 1 PDLMICAD / Se modifica el apartado primero del artículo 20, primero por el artículo 8 DLCAD, y, después, por la letra a) del apartado primero del artículo 13 PDLMICAD / Se incorpora el apartado primero bis del artículo 20 por el artículo 8 DLCAD, después sustituido por la letra b) del apartado primero del artículo 13 PDLMICAD / Se modifica el apartado 3 del artículo 20, primero por el artículo 8 DLCAD, y, después, por la letra d) del apartado primero del artículo 13 PDLMICAD, siendo necesario acudir también al respecto al apartado 6 DPRDA / Se incorpora el apartado 5 bis del artículo 20 por la letra a) del apartado primero del artículo 13 PDLMICAD / Se sustituye la rúbrica del artículo 21 por la letra a) del apartado primero del artículo 14 PDLMICAD / Se modifica el apartado primero del artículo 21 por el artículo 9 DLCAD / Se modifica el apartado segundo del artículo 21, primero por el artículo 9 DLCAD, y, después, con los actuales apartados 2 y 2 bis, por la letra b) del apartado primero del artículo 14 PDLMICAD / Se incluye un apartado 2 bis al artículo 21 por la letra b) del apartado primero del artículo 14 PDLMICAD / Se modifica el artículo 23, primero por el artículo 11 DLCAD, y, después, por el apartado duodécimo del artículo 16 DLMU, siendo sustituido por el apartado primero del artículo 16 PDLMICAD / Se incorpora el artículo 23 bis por el apartado segundo del artículo 16 |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| | | | | | | | | | PDLMICAD / Se incorpora el artículo 23 ter por el apartado segundo del artículo 16 PDLMICAD, siendo necesario acudir también al respecto al apartado 8 del artículo 57 de dicho PDLMICAD / Se incorpora el artículo 23 quater por el apartado 2 PDLMICAD / Se sustituye el artículo 25 por el apartado segundo del artículo 17 PDLMICAD |
| | | | | | | 6.6 (52) | - | 21.5 | Se sustituye la rúbrica del artículo 21 por la letra a) del apartado primero del artículo 14 PDLMICAD |
| Registro de PSSIic | - | 7 (11) | - | E.M.III.4º (34) | - | - | - | - | - |
| Certificados electrónicos de personas jurídicas | - | - | - | 7 | Se modifica el apartado 2 del artículo 7 por la D. F. 4.3 LMSO | - | - | - | - |
| Extinción de la vigencia de los certificados electrónicos | - | 9.1, 9.2 y 9.3 | - | 8 (35) | Se modifica el apartado 2 del artículo 8 por la D. F. 6 LGT | - | - | 21.3 y 36 | Se sustituye la rúbrica del artículo 21 por la letra a) del apartado primero del artículo 14 PDLMICAD / Se modifica la letra a) del apartado primero del artículo 36 por el artículo 16 DLCAD |
| Suspensión de la vigencia de los certificados electrónicos | - | 9.4 | - | 9 (36) | - | - | - | | |
| Disposiciones comunes a la extinción y suspensión de la vigencia de los certificados electrónicos | - | - | - | 10 | - | - | - | | |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| Requisitos de los certificados electrónicos reconocidos | Anexo I | 8 | - | 11.2, 11.3 y 11.4 | - | - | - | 28 y 33 | Se modifica la letra g) del apartado primero del artículo 28 por el artículo 12 DLCAD / Se modifica el apartado tercero, en su enunciado, letra a) y letra b), del artículo 28 por el artículo 12 DLCAD / Se incorpora un apartado 3 bis al artículo 28 por el apartado primero del artículo 19 PDLMICAD, siendo necesario acudir también al respecto al apartado noveno del artículo 57 de PDLMICAD |
| Obligaciones previas a la expedición de certificados electrónicos reconocidos | - | 11.a) (12) | - | 12 | Se modifica el apartado c) del artículo 12 por la D. F. 4.4 LMSO | - | - | - | - |
| Comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido | - | - | - | 13 | Se modifican los apartados 2 y 3 del artículo 13 por el artículo 5.3 LMISI | - | - | - | - |
| Equivalencia internacional de certificados reconocidos | 7 | 10 (13) | - | 14 (37) | - | 6.5 | - | 21.4 | Se sustituye la rúbrica del artículo 21 por la letra a) del apartado primero del artículo 14 PDLMICAD |
| DNIe | - | - | - | 15 | - | 8 y 9.1 | El artículo 8.1 DLDFE sustituye al artículo 36.1 DPRDA. El artículo 8.2 DLDFE sustituye el artículo 36.e), apartado tercero, DPRDA. El artículo 8.3 DLDFE sustituye los apartados 4 y 5 del artículo 36 DPRDA. El artículo 9 DLDFE sustituye al artículo 38.2 DPRDA | 1.c) y 66 | Se modifica el apartado c) del artículo 1 por la letra b) del apartado primero del artículo 1 PDLMICAD / Se modifican los apartados primero, tercero y cuarto del artículo 66 por el artículo 48 PDLMICAD / Se introduce el apartado 8 bis por el apartado 1 del artículo 37 LSESCPC, después modificado por el apartado 101 del artículo 2 LFBAPS (Gazzetta Ufficiale num. 302, 30 dicembre 2009) |
| Requisitos y características del DNIe | - | - | - | 16 | - | | | | |
| Obligaciones del titular del certificado | - | - | - | 23.1 | Se modifican los apartados 1.c) y d) del artículo 23 por la D. F. 4.8 LMSO | - | - | 32.1 | Se modifica este apartado primero del artículo 32 por el artículo 14 DLCAD |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| Protección de los datos personales | 8 | 15 (14) | - | 17 (38) | - | - | - | 32.5 y 33 | - |
| Obligaciones de los PSSIic que expidan certificados electrónicos | - | 11 (15) | - | 18 | Se modifican los apartados a) y b) del artículo 18 por la D. F. 4.5 y 4.6 LMSO | - | - | 32.2 y 32.4 | Se modifica el apartado segundo del artículo 32 por el artículo 14 DLCAD |
| Declaración de prácticas de certificación | - | - | - | 19 | - | - | - | - | - |
| Obligaciones de los PSSIic que expidan certificados electrónicos reconocidos | Anexo II | 12 (16) | - | 18.b), 20 y 28.1 (39) | Se modifican los apartados a) y b).1.º del artículo 18 por la D. F. 4.5 y 4.6 LMSO / Se modifica el apartado 1.e) del artículo 20 por la D. F. 4.7 LMSO | - | - | 27 y 32.3 (55) | Se modifican los apartados tercero y cuarto del artículo 27 en los términos de cuanto se ha dispuesto por el apartado 18 del artículo 57 PDLMICAD / Se suprime la letra f) del apartado tercero del artículo 32 por la letra a) del apartado primero del artículo 22 PDLMICAD / Se modifica la letra j) del apartado tercero del artículo 32 por el artículo 14 DLCAD / Se incorpora una letra m bis al apartado tercero del artículo 32 por la letra b) del apartado primero del artículo 22 PDLMICAD |
| Cese de la actividad de los PSSIic | - | 13 | - | 21 | - | - | - | 37 | Se modifican los apartados primero y cuarto del artículo 37 en los términos de cuanto se ha dispuesto por el apartado 18 del artículo 57 PDLMICAD / Se incorpora un apartado 4 bis al artículo 37 por el apartado primero del artículo 25 PDLMICAD |
| Responsabilidad de los PSSIic | 6 | 14 (17) | - | 22 (40) | - | 7 | Este precepto introduce el artículo 28 bis DPRDA | 30.1 y 30.2 | - |
| Limitaciones de responsabilidad de los PSSIic | - | 14.2 | - | 23 (41) | Se modifica el apartado 5 del artículo 23 por el artículo 5.4 LMISI /Se modifican los apartados 1.c) y d) del artículo 23 por la D. F. 4.8 LMSO | - | - | 30.3 | Se modifica este apartado tercero del artículo 30 por el artículo 13 DLCAD |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| Certificación de PSSIic | 3.2 | 6 | - | 26 (42) | - | 2.1.c) y 5 | - | 29 | Se modifica los apartados primero, quinto y noveno del artículo 29 en los términos de cuanto se ha dispuesto en el apartado 18 del artículo 57 PDLMICAD / Se modifica el apartado octavo del artículo 29 por el apartado primero del artículo 20 PDLMICAD |
| Requisitos de los dispositivos seguros de creación de firma electrónica | Anexo III | 19 (18) | - | 24.3, *in fine*, y 28.1 | - | 10 | - | 35 | Se sustituyen los apartados tercero y cuarto del artículo 35 por la letra a) del apartado primero del artículo 24 PDLMICAD / Se modifica el apartado quinto del artículo 35 por los números 1) y 2) de la letra b) del apartado primero del artículo 24 PDLMICAD / Se sustituye el apartado sexto del artículo 35 por la letra c) del apartado primero del artículo 24 PDLMICAD |
| Certificación de dispositivos seguros de creación de firma electrónica | 3.4 y 3.5 | 20 y 21 (19) | - | 27 y 28.2 (43) | - | - | - | | |
| Requisitos de los dispositivos de verificación de firma electrónica | Anexo IV | 22 (20) | - | 25.3 y 25.4 (44) | - | - | - | 33 | Se modifica el apartado primero del artículo 33 por el apartado primero del artículo 23 PDLMICAD |
| Supervisión y control | 3.3 | 16 (21) | - | 29 (45) | Se añade el apartado 5 al artículo 29 por la D. F. 4.9 LMSO | 4 | - | 31 | Se sustituye el artículo 31 por el apartado primero del artículo 21 PDLMICAD |
| Deber de información y colaboración | - | 17 (22) | - | 30 (46) | - | - | - | - | - |
| Resoluciones del órgano de supervisión | - | 18 | - | - | - | - | - | - | - |
| Régimen aplicable a la tasa de los artículos 6, 21 y 22 RDLFE | - | 23 | - | - | - | - | - | - | - |
| Infracciones | - | 24 y 25 (23) | - | 31 | Se modifica el apartado 4 del artículo 31 por el artículo 5.5 LMISI | - | - | - | - |
| Sanciones | - | 26 | - | 32 | - | - | - | 32 bis | Se incorpora el artículo 32 bis por el apartado segundo del artículo 22 PDLMICAD |
| Graduación de la cuantía de las sanciones | - | - | - | 33 (47) | - | - | - | - | - |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| Medidas cautelares | - | 27 | - | 34 | - | - | - | - | - |
| Multa coercitiva | - | - | - | 35 | - | - | - | - | - |
| Competencia y procedimiento sancionador | - | 28 | - | 36 | - | - | - | - | - |
| Comité | 9 | - | - | - | - | - | - | - | - |
| Funciones del Comité | 10 | - | - | - | - | - | - | - | - |
| Notificación | 11 | - | - | - | - | - | - | - | - |
| Revisión | 12 | - | - | - | - | - | - | - | - |
| Aplicación | 13 | - | - | - | - | - | - | - | - |
| Destinatarios | 15 | - | - | - | - | - | - | - | - |
| Posibilidad de emisión por las entidades públicas de radiodifusión de una Comunidad Autónoma en el territorio de otras con las que aquella tenga espacios radioeléctricos colindantes | - | D. A. Única | - | - | - | - | - | - | - |
| Firma electrónica pública y uso de firma electrónica | - | 1.2.1º | - | D. A. 1ª | - | - | | - | - |
| Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica | - | - | - | D. A. 2ª | - | - | - | - | - |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias | - | - | - | D. A. 3ª | - | - | - | - | - |
| PSSIic por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda | - | - | - | D. A. 4ª | - | - | - | - | - |
| Modificación del artículo 81 PLMFAOS (BOE núm. 313, de 31 de diciembre de 1997) | - | - | - | D. A. 5ª | - | - | - | - | - |
| Régimen jurídico del DNIe | - | - | - | D. A. 6ª | - | - | - | - | - |
| Emisión de facturas por vía electrónica | - | - | - | D. A. 7ª | - | - | - | - | - |
| Modificaciones de la LSSICE | - | - | - | D. A. 8ª | - | - | - | - | - |
| Garantía de accesibilidad para las personas con discapacidad y de la tercera edad | - | - | - | D. A. 9ª | - | - | - | - | - |
| Modificación de la LECiv. | - | - | - | D. A. 10ª | - | - | - | - | - |
| Resolución de conflictos | - | - | - | D. A. 11ª | Se añade la D.A. 11ª por el artículo 5.6 LMISI | - | - | - | - |
| PSSIic establecidos en España antes de la entrada en vigor de este RDLFE | - | D. T. Única | - | - | - | 11.2 y 11.3 | - | - | - |

| Concepto | UE | España | | | | Italia | | | |
|---|---|---|---|---|---|---|---|---|---|
| | DFE | RDLFE | | LFE | | DLDFE | | CAD | |
| | Artículos | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) | Artículos | Modificaciones (antes RIE-SCTE) |
| Validez de los certificados electrónicos expedidos previamente a la entrada en vigor de la LFE | - | - | - | D. T. 1ª | - | - | - | 72 | - |
| PSSIic establecidos en España antes de la entrada en vigor de la LFE | - | - | - | D. T. 2ª | - | - | - | - | - |
| Actualizaciones | - | - | - | - | - | - | - | 73 | - |
| Gastos financieros | - | - | - | - | - | - | - | 74 | - |
| Derogación normativa | - | - | - | D. D. Única | - | - | - | 75 | Se incorpora un apartado 3 bis al artículo 75 por el apartado primero del artículo 54 PDLMICAD |
| Fundamento constitucional | - | D. F. 1ª | - | D. F. 1ª (48) | - | - | - | - | - |
| Habilitación al Gobierno | - | D. F. 2ª | - | D. F. 2ª | - | - | - | - | - |
| Entrada en vigor | 14 | D. F. 3ª | - | D. F. 3ª | - | 13 | - | 76 | - |

*Anexo XIV. La Directiva sobre firma electrónica y su transposición al ordenamiento jurídico interno, español e italiano. Fuente: elaboración propia*

(1) El artículo 1.1, *in fine*, RDLFE no contempla la aplicación del RDLFE a los SSIic prestados por los PSSIic, a diferencia de la DFE (artículo 4.1, *ab initio*). Además, el artículo 1.1 RDLFE (que coincide con el artículo 1.1 DFE) establece el mismo ámbito de aplicación que el artículo 2.1 LSSICE. En este caso, entiendo que, para saber a qué normativa estarán sujetos 1) los SSIic prestados por los PSSIic establecidos en España, 2) los SSIic que los PSSIic residentes o domiciliados en otro Estado miembro de la UE/EEE ofrezcan a través de un establecimiento permanente situado en España, 3) los PSSIic establecidos en otro Estado miembro de la UE/EEE cuando el DSSIic (tercero que confía) radique en España y los SSIic afecten a materias concretas y 4) los PSSIic establecidos en países que no sean miembros de la UE/EEE, se estará a lo dispuesto en los artículos 2.2, 3 y 4 LSSICE; el motivo de esta aplicación subsidiaria, a mi juicio, es que la naturaleza de los PSSIic es la de PSSIi. Por último, el artículo 1.2 RDLFE coincide con el artículo 1.2 DFE.

(2) El artículo 2.a) RDLFE habla de la firma electrónica como medio de identificación, mientras que el artículo 2.1) DFE habla de la firma electrónica como medio de autenticación. Me parece más adecuada la definición del artículo 2.a) RDLFE, ya que entiendo que la firma electrónica, más que un medio de autenticación, es un medio de identificación. La autenticación se consigue cuando, existente la identificación, el PSSIic acredita que el signatario es quien dice ser.

(3) La DFE utiliza el término firmante, mientras que el RDLFE el de signatario.

(4) La DFE permite que tanto personas físicas como personas jurídicas puedan ser titulares de firma electrónica. En cambio, el RDLFE sólo permite que puedan ser titulares de firma electrónica las personas físicas. Asimismo, la DFE establece que el firmante puede actuar en nombre de una entidad, mientras que el RDLFE no. El RDLFE sólo permite a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos (artículo 5.3, *in fine*, RDLFE).

(5) El RDLFE establece que el certificado debe estar referido al signatario (firmante), mientras que la DFE no exige que sea firmante, sino que puede estar vinculado a cualquier persona.

(6) Según la DFE, puede ser PSSIic una entidad, una persona física o una persona jurídica, mientras que el RDLFE sólo contempla que pueda serlo una persona física o una persona jurídica. Además, según el RDLFE, ha de existir, siempre, la actividad certificadora, sin perjuicio de que, además, se presten otros servicios. Sin embargo, la literalidad de la DFE permite interpretar, sobre la base de la disyuntiva *o*, que la actividad puede ser la de certificación o bien otra relacionada con la firma electrónica, de modo que, aun cuando no se emitiesen certificados, se trataría de un PSSIic.

(7) La DFE habla de que la acreditación voluntaria consistirá en un permiso que se concederá por un organismo público o privado, mientras que el RDLFE sólo habla de organismo público. Por otro lado, la DFE dice que ese organismo estará encargado del establecimiento y supervisión del cumplimiento de los derechos y obligaciones establecidos por el permiso, mientras que el RDLFE sólo dice que el organismo en cuestión será el encargado de la supervisión (no, además, como la DFE, de su establecimiento). Por último, la DFE añade que este permiso se concederá «cuando el proveedor de servicios de certificación no esté habilitado para ejercer los derechos derivados del permiso hasta que haya recaído la decisión positiva de dicho organismo», mientras que el RDLFE no añade esta exigencia.

(8) El artículo 4.1, *ab initio*, RDLFE se corresponde con el artículo 3.1 DFE. Por su parte, el artículo 4.1, *in fine*, RDLFE se corresponde con el artículo 4.1, *in fine*, DFE. Finalmente, el artículo 4.2 RDLFE no tiene equivalente en la DFE.

(9) El artículo 4.1, *ab initio*, DFE se corresponde con el artículo 1.1, *in fine*, RDLFE. El artículo 4.1, *in fine*, DFE se corresponde con el artículo 4.1, *in fine*, RDLFE. El artículo 4.2 DFE no tiene equivalente en el RDLFE.

(10) El artículo 3.1.1º RDLFE se corresponde con el artículo 5.1 DFE, si bien incorpora un artículo 3.1.2º RDLFE que no se encuentra en la DFE. A su vez, el artículo 3.2 RDLFE se corresponde con el artículo 5.2 DFE, pese a que esta última añade que esta exclusión no se producirá respecto de la firma electrónica avanzada, mientras que el RDLFE parece ser más adecuado, al referirse a la firma electrónica en general, sin especificar los requisitos de la firma electrónica avanzada. Además, el artículo 3.1, *in fine*, RDLFE añade que este tipo de firma electrónica (que equivale, en términos de la LFE, a la firma electrónica reconocida), se valorará según los criterios de apreciación establecidos en las normas procesales, previsión esta que no consta en la DFE.

(11) Difícil encuadre de este registro con el principio de no autorización previa, entre otras cosas porque lo que exige la DFE es la notificación por los Estados miembros de los PSSIic nacionales que se hayan inscrito en el sistema de acreditación voluntaria –artículo 11.1.c) DFE–, no la notificación de todos los PSSIic. Estas obligaciones tendrán que cumplirse cumulativamente con las contenidas en la DCE, en la LSSICE, en el TRLGDCU y (si el PSSIic emite certificados reconocidos) las contenidas en el artículo 12 RDLFE.

(12) El artículo 11.a) RDLFE sólo se corresponde con el artículo 12.a) LFE. No obstante, el artículo 11.a) RDLFE se refiere a todo tipo de certificados (reconocidos o no), mientras que el artículo 12.a) LFE se refiere sólo a los certificados reconocidos.

(13) Sólo el artículo 7.1 DFE. Sabemos que los certificados reconocidos expedidos por un PSSIic establecido en un país fuera de España y de la UE/EEE se reconocerán como jurídicamente como equivalentes a los expedidos por un PSSIic establecido en España (artículo 10 RDLFE); ahora bien, ¿cabe entender que, como en virtud del artículo 4.1 RDLFE, no se pueden establecer restricciones a la prestación de SSIic de PSSIic establecidos fuera de España pero dentro de la UE/EEE, los certificados (reconocidos y no reconocidos) expedidos por estos PSSIic establecidos en un Estado miembro distinto a España pero dentro de la UE/EEE deberán ser reconocidos en España como jurídicamente equivalentes a los certificados (reconocidos y no reconocidos) expedidos por PSSIic establecidos en España? Entiendo que sí. De ser así, la diferencia entre los PSSIic establecidos fuera de España y de la UE/EEE y los PSSIic establecidos fuera de España y fuera de la UE/EEE sería que los primeros pueden reconocer válidamente certificados reconocidos y no reconocidos en España (y viceversa), mientras que los segundos sólo pueden reconocer certificados reconocidos. Por último, el artículo 7.2 y 7.3 DFE no tienen equivalente en el RDLFE, algo lógico, ya que ambos apartados se refieren a las obligaciones de la Comisión.

(14) El artículo 8.2 DFE añade que «los datos no podrán obtenerse o tratarse con fines distintos sin el consentimiento explícito de su titular», de modo que deja abierta la puerta, entiendo, a que puedan obtenerse o tratarse con fines distintos con el consentimiento de su titular; el RDLFE, en cambio, no contempla esta posibilidad. Además, el RDLFE (artículo 8.3) exige, en los supuestos de uso de seudónimo, constatar la verdadera identidad del signatario y conservar la documentación que la acredite; la DFE no prevé esta exigencia.

(15) Difícil encuadre de este registro con el principio de no autorización previa, entre otras cosas porque lo que exige la DFE es la notificación por los Estados miembros de los PSSIic nacionales que se hayan inscrito en el sistema de acreditación voluntaria –artículo 11.1.c) DFE–, no la notificación de todos los PSSIic. Estas obligaciones tendrán que cumplirse cumulativamente con las contenidas en la DCE, en la LSSICE, en el TRLGDCU y (si el PSSIic emite certificados reconocidos) las contenidas en el artículo 12 RDLFE.

(16) De este modo, los PSSIic que expidan certificados reconocidos, tendrán que cumplir cumulativamente las obligaciones contenidas en los artículos 11 y 12 RDLFE (además de las obligaciones de los PSSI y de los PSSIi contenidas en la DCE, en la LSSICE y en el TRLGDCU).

(17) Si bien la DFE exige un mínimo de responsabilidad, que será aquella que recaiga en los PSSIic que expiden certificados reconocidos (artículo 6 DFE), el RDLFE va más allá y contempla una responsabilidad general para los PSSIic que expiden certificados reconocidos y no reconocidos. Esta responsabilidad, si se cumple mi idea de que los PSSIic tienen la naturaleza de PSSIi, deberá aplicarse cumulativamente junto con la establecida en la DCE y en la LSSICE para PSSI y PSSIi.

(18) El artículo 19.2º RDLFE exige que exista seguridad razonable de que los datos utilizados para la generación de firma electrónica no puedan ser derivados de los datos de verificación de firma electrónica, mientras que el anexo.1.b) habla de que estos datos no puedan ser hallados por deducción.

(19) *Vid.* DCMO y DPNRNPFE.

(20) El apartado a) del anexo IV DFE no tiene su equivalente en el artículo 22 RDLFE.

(21) El artículo 3.3 DFE sólo exige esta supervisión respecto de los PSSIic que expidan certificados reconocidos. El RDLFE amplia esta supervisión también, en los supuestos indicados, a los PSSIic que expidan certificados no reconocidos.

(22) *Vid.* artículos de la DCE y de la LSSICE sobre deber de colaboración de los PSSI (incluidos PSSIi). Y es que, si se cumple la teoría de que los PSSIic tienen la naturaleza de PSSIi, deberá aplicarse cumulativamente junto con la establecida en la DCE (artículo 19) y en la LSSICE (artículos 11 y 36) para PSSI y PSSIi.

(23) Si se cumple mi idea de que los PSSIic tienen la naturaleza de PSSIi, deberá aplicarse cumulativamente junto con la establecida en la DCE y en la LSSICE en materia de infracciones y sanciones para PSSI y PSSIi. Lo mismo cabría decir de los artículos 26, 27 y 28 RDLFE.

(24) El artículo 1.1 LFE coincide con el artículo 1.1º DFE y con el artículo 1.1, *ab initio*, RDLFE. El artículo 1.2 LFE coincide con el artículo 1.2º DFE y con el artículo 1.2.1º RDLFE. El artículo 2.1 LFE coincide con el artículo 4.1, *ab initio*, DFE y con el artículo 1.1, *in fine*, RDLFE, si bien amplía el ámbito de aplicación, ya que el RDLFE establecía su aplicación sólo a los PSSIic establecidos en España, mientras que la LFE (en línea con el artículo 2 LSSICE) establece que la LFE se aplicará, no sólo a los PSSIic establecidos en España, sino también a los SSIic que los residentes o domiciliados en otro Estado miembro de la UE/EEE ofrezcan a través de un establecimiento permanente situado en España. Desconozco por qué no incluye, como sí hace el artículo 2.1 LSSICE, a los SSIic prestados por los PSSIic establecidos en España. Asimismo, el artículo 2.3 LFE no tiene equivalente ni en la DFE ni en el RDLFE, coincidiendo literalmente con el artículo 2.1.2º LSSICE. De igual modo, el artículo 2.4 LFE no tiene equivalente ni en la DFE ni en el RDLFE, coincidiendo literalmente con el artículo 2.2.2º LSSICE. Lo mismo sucede con el artículo 2.5 LFE, que no tiene equivalente ni en la DFE ni en el RDLFE, coincidiendo literalmente con el artículo 2.3. LSSICE.

(25) El artículo 3.1 LFE habla de la FE como medio de identificación, mientras que el artículo 2.1) DFE habla de la FE como medio de autenticación.

(26) Con respecto a la DFE, el artículo 3.2 LFE dice que la firma electrónica avanzada ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, mientras que la DFE dice que la firma electrónica avanzada ha sido creada por medios que el firmante puede mantener (no añade con un alto nivel de confianza, como sí hace la LFE) bajo su control exclusivo. Con respecto al RDLFE, la LFE dice que la firma electrónica avanzada ha sido creada por medios que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, mientras que el RDLFE dice que la firma electrónica avanzada ha sido creada por medios que el firmante mantiene (no utiliza –LFE– ni puede mantener –DFE–) bajo su control exclusivo (tampoco añade con un alto nivel de confianza, como sí hace la LFE).

(27) Desaparece la afirmación contenida en el RDLFE de que sólo las personas físicas pueden ser titulares de firma electrónica; ahora, en línea con la DFE, pueden ser titulares de firma electrónica tanto las personas físicas como las personas jurídicas. La LFE dice que el firmante será la persona (física o jurídica) que utiliza un dispositivo de creación de firma electrónica, no exigiendo que esté en posesión de él (como sí lo hace la DFE) ni que cuente con él (como sí lo hace el RDLFE). Por último, la LFE, al igual que el RDLFE, dice que el firmante podrá actuar en nombre propio o en nombre de una persona física o jurídica a la que representa, mientras que la DFE añade que el firmante, además de actuar en nombre propio o en nombre de una persona física o jurídica a la que representa, también podrá actuar en nombre de una *entidad*.

(28) La LFE, con respecto a la DFE y al RDLFE, sustituye el término *aparato informático* por el de *sistema informático*.

(29) Al igual que la DFE y el RDLFE, la LFE incluye como posibles PSSIic a personas físicas y jurídicas; sólo la DFE incluye el término también a las *entidades*. No obstante, la LFE se separa del criterio del RDLFE y se acerca a la DFE al establecer que la expedición de certificados no es necesaria, sino alternativa, de modo que podrán ser PSSIic aquellas personas físicas o jurídicas que no expidan certificados, siempre que realicen otros SSIic en relación con la firma electrónica. Por su parte, el artículo 2.3, 2.4 y 2.5 LFE no tiene equivalente ni en la DFE ni en el RDLFE, coincidiendo literalmente con el artículo 2.1.2º LSSICE, 2.2.2º y 2.3 LSSICE.

(30) El artículo 5.1 LFE coincide con el artículo 3.1 DFE y 4.1 RDLFE. Por su parte, el artículo 5.2 LFE no tiene equivalente ni en la DFE ni en el RDLFE. Por último, el artículo 5.3 LFE no tiene equivalente en la DFE y coincide con el artículo 4.2, *in fine*, RDLFE, si bien este último artículo contiene una parte *ab initio*, no recogida en la LFE, donde establece que esta actividad «se realizará con la debida separación de cuentas».

(31) El artículo 4.1.1º Y 4.1.2º LFE coincide con el artículo 3.7, *ab initio*, DFE y con el artículo 5.1.1º y 5.1.2º RDLFE. El artículo 4.2 LFE coincide con el artículo 3.7, *in fine*, DFE y con el artículo 5.1.3º y artículo 5.2 RDLFE, si bien la LFE sustituye el término *Administraciones públicas extranjeras* empleado por el RDLFE (que abarcaba a las Administraciones públicas que estuvieran fuera de España, ya sea dentro o fuera de la UE/EEE) por el de *Administraciones públicas del EEE*, que abarca sólo a las Administraciones públicas que estuvieran fuera de España pero dentro del EEE (la LFE sustituye, simultáneamente, el término *UE/EEE* por el sólo de *EEE*). El artículo 4.3 LFE no tiene equivalente en la DFE y coincide con el artículo 5.1.3 RDLFE, si bien, mientras que el RDLFE exigía que se dicten a propuesta del Ministerio de Administraciones Públicas únicamente, la LFE exige que se dicten a propuesta conjunta del Ministerio de Administraciones Públicas y del Ministerio de Ciencia y Tecnología (nada que decir respecto del informe previo, ya que, en ambos casos, es el mismo –Consejo Superior de Informática, después llamado Consejo Superior de Informática y para el impulso de la Administración Electrónica–). El artículo 4.4 LFE no tiene equivalente en la DFE y coincide con el artículo 5.3 RDLFE, si bien se elimina la parte final de este último artículo, que disponía que «[a]simismo, el Ministerio de Economía y Hacienda, respetando las condiciones previstas en este RDLFE, podrá establecer un régimen normativo destinado a garantizar el cumplimiento de las obligaciones tributarias, determinando, respecto de la gestión de los tributos, la posibilidad de que el signatario sea una persona física o una persona jurídica»; la razón de esta última derogación se explica en el apartado tercero de la Exposición de Motivos, párrafos 11º, 12º, 13º y 16º y D. A. 3ª (esta última para la expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias), de la LFE.

(32) El artículo 5.1 LFE coincide con el artículo 4.1, *in fine*, DFE y con el artículo 4.1 RDLFE. El artículo 4.1, *ab initio*, DFE y el artículo 1.1, *in fine*, RDLFE coinciden con el artículo 2 LFE.

(33) Sólo el artículo 5.1.a), 5.1.b) y 5.2 DFE. A diferencia de la DFE y del RDLFE, la LFE (artículo 3.3) incorpora por primera vez el término *firma electrónica reconocida*, coincidiendo su significado con el contenido del artículo 5.1, *ab initio*, DFE y con el artículo 3.1.1º RDLFE. El artículo 3.4 LFE coincide con el artículo 5.1.a) DFE y con el artículo 3.1.1º RDLFE. El artículo 3.5.1º LFE, que no tiene equivalente ni en la DFE ni en el RDLFE, incorporando por primera vez una definición de *documento electrónico*, habría que poner en relación con cuanto dispone el artículo 24 LSSICE para una modalidad concreta de documento electrónico, cual es el contrato electrónico; el artículo 3.5.2º LFE, que, no tendiendo equivalente ni en la DFE ni en el RDLFE, habla de los requisitos que habrá de satisfacer dicho documento electrónico para tener la naturaleza de documento público –que serán los requisitos del artículo 3.6.a) LFE y, en su caso, los contenidos en la normativa aplicable–, de documento administrativo –que serán los requisitos del artículo 3.6.b) LFE y, en su caso, los contenidos en la normativa aplicable– y de documento privado –que serán los del artículo 3.6.c) LFE–. El artículo 3.7 LFE, que no tiene equivalente ni en la DFE ni en el RDLFE, habla del valor y de la eficacia de los distintos tipos de documentos contenidos en el artículo 3.6.a), 3.6.b) y 3.6.c) LFE. El artículo 3.8, *ab initio*, LFE coincide con el artículo 5.1.b) DFE y con el artículo 3.1.1º RDLFE, si bien, mientras que la DFE y el RDLFE hablan de la admisión como prueba en procedimientos judiciales de la (en términos de la posterior LFE) firma electrónica reconocida, la LFE habla de la admisión como prueba en procedimientos judiciales del soporte en que se hallen los datos firmados electrónicamente, es decir, del documento con firma electrónica, de modo que ahí se podrían incluir (a diferencia de la DFE y del RDLFE) la firma electrónica simple o general y la firma electrónica avanzada. Por lo demás, el resto del artículo 3.8.1º, así como el artículo 3.8.2º y el artículo 3.8.3º LFE, hablan de cómo se ha de proceder cuando se impugne la autenticidad de la firma electrónica avanzada y de la firma electrónica reconocida, no incluyéndose disposición alguna que indique cómo se ha de proceder si se impugnase la autenticidad de la firma electrónica simple o general (que, no obstante, entiendo, requeriría del mismo proceder que con respecto a la firma electrónica avanzada). El artículo 3.9 LFE coincide con el artículo 5.2 DFE y con el artículo 3.2 RDLFE, si bien el primero habla de que no se negarán efectos jurídicos a la firma electrónica que no reúna los requisitos de firma electrónica reconocida por el mero hecho de presentarse en forma electrónica, mientras que el segundo añade que no sólo no se le negarán efectos jurídicos, sino que tampoco se le negará su admisibilidad como prueba en procedimientos judiciales (esta previsión no la recoge la LFE pero, entiendo, se hallaría incluida en el artículo 3.8, *ab initio*, LFE), añadiendo, a diferencia de la LFE, que no se producirán estos efectos por el mero hecho de que se presente en forma electrónica (esta previsión sí se contiene en el artículo 3.9 LFE), no se base en un certificado reconocido (esta previsión se contiene en el artículo 3.3 LFE y en el artículo 3.1.1º y 3.1.2º RDLFE), no se base en un certificado expedido por un PSSIic acreditado (esta previsión no se contiene en la LFE pero sí en el artículo 3.1.2º RDLFE) o no esté creada por un dispositivo seguro de creación de firma electrónica (esta previsión se contiene en el artículo 3.3 LFE y en el artículo 3.1.1º y 3.1.2º RDLFE). El artículo 3.10 LFE habla del uso de firma electrónica (cualquiera que sea su modalidad) conforme a las condiciones acordadas por las partes para relacionarse entre sí, donde se tendrá en cuenta lo estipulado entre ellas; este artículo coincide con lo dispuesto en el considerando 16 DFE, no teniendo equivalente en el RDLFE. El artículo 3.11 LFE, por último, habla de los efectos jurídicos plenos de los sistemas de identificación y firma electrónica previstos en la Ley de procedimiento administrativo común de las Administraciones públicas y en la Ley de régimen jurídico del sector público, sin que este artículo tenga equivalente ni en la DFE ni en el RDLFE.

(34) Este registro desaparece con la LFE.

(35) El artículo 8.1.a) LFE coincide con el artículo 9.1.a), *ab initio*, RDLFE. Se añade, respecto del artículo 9.1.b) RDLFE, un inciso final al apartado b) del artículo 8 LFE, en coherencia con lo dispuesto en el artículo 7 LFE. El artículo 8.1.c) LFE engloba el anterior apartado d) del artículo 9.1 RDLFE, mientras que el apartado c) del artículo 9.1 RDLFE no tiene equivalente en el artículo 8.1 LFE. Los apartados d) y e) de los artículos 8.1 LFE y 9.1 RDLFE coinciden. Los artículos e) del artículo 8.1 LFE y f) del artículo 9.1 RDLFE, con las salvedades oportunas derivadas de la incorporación de las personas jurídicas como posibles firmantes, también coinciden. Los artículos f) del artículo 8.1 LFE y g) del artículo 9.1 RDLFE también coinciden. El apartado g) del artículo 8.1 LFE habla de alteración o modificación de las circunstancias, mientras que el artículo 9.1.h) RDLFE habla de inexactitudes. Se incorpora un apartado h) al artículo 8.1 LFE que no tiene su equivalente en el RDLFE. El artículo 8.2 LFE coincide con el artículo 9.1.a), *in fine*, RDLFE, si bien en la LFE se amplía el período máximo de validez de los certificados reconocidos, que pasa de 4 a 5 años. El artículo 8.3 LFE coincide con el artículo 9.2 RDLFE, si bien con la LFE sólo la expiración del período de validez –apartado a) del artículo 8.1 LFE– surtirá efectos desde el momento en que se produzca esta circunstancia, mientras que, en los demás casos, lo hará desde que la indicación de la causa de extinción se incluya en el servicio de consulta sobre la vigencia de los certificados (reconocidos o no) del PSSIic; en cambio, en el RDLFE, no sólo la expiración del período de validez surtirá efectos desde el momento en que se produzca, sino también el supuesto de cese de actividad del PSSIic –apartados a) y g) del artículo 9.1 RDLFE, apartados a) y f) del artículo 8, apartado 1, LFE–, mientras que, en los demás casos, lo hará desde la fecha en que el PSSIic tenga conocimiento cierto de cualquiera de los hechos determinantes de ella y así lo haga constar en el registro de certificados a que se refiere el artículo 11.e) RDLFE. No consta en el artículo 8 LFE el equivalente al artículo 9.3 RDLFE. Por último, el equivalente al apartado 4 del artículo 9 RDLFE consta en el artículo 9 LFE.

(36) El artículo 9 (apartados 1 y 2) LFE coincide con el artículo 9.4 RDLFE, si bien la LFE adapta el apartado a) a las nuevas circunstancias (como la prevista por el artículo 7 LFE) e incluye dos nuevos apartados –c) y d)– no previstos en el RDLFE. El artículo 9.2 LFE clarifica el momento a partir del cual la suspensión de la vigencia de un certificado electrónico (reconocido o no) surtirá efectos, ya que en el artículo 9.4, *in fine*, RDLFE no quedaba claro, al hacer una remisión un tanto confusa.

(37) El artículo 14.b) LFE añade, respecto a la DFE y al RDLFE, la exigencia de que el PSSIic que garantice el certificado reconocido cumpla los requisitos establecidos en la normativa comunitaria en materia de firma electrónica para la expedición de certificados reconocidos, de modo que antes podía estar garantizada por un PSSIic que cumpliera los requisitos establecidos en la normativa comunitaria sobre firma electrónica (fuera para la expedición de certificados reconocidos o para la expedición de certificados no reconocidos) y ahora sólo se permite que el certificado reconocido esté garantizado por un PSSIic que cumpla la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

(38) El artículo 17.2.2º LFE retoma la previsión contenida en la DFE, no recogida en el RDLFE, de que «los datos no podrán tratarse con fines distintos sin el consentimiento explícito de su titular», si bien no incluye el término *obtenerse*, como sí hace la DFE, de modo que deja abierta la posibilidad a que puedan obtenerse con fines distintos sin el consentimiento explícito de su titular. Por último, a diferencia del artículo 15.3, *in fine*, RDLFE, se elimina la previsión que decía que «ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas».

(39) El artículo 18.b) LFE viene a desarrollar lo que, antes, de manera ciertamente escueta, se contemplaba en el artículo 11.d) y 12.i) RDLFE. Por lo que respecta al artículo 20 LFE, se elimina lo dispuesto por el artículo 12.c) y 12.k) RDLFE.

(40) El artículo 22.1 LFE se corresponde con el artículo 14.1 y 14.3 RDLFE, si bien ha eliminado dos importantes previsiones, contempladas en el artículo 14.1 RDLFE («o actúen con negligencia») y en el artículo 14.3, *in fine*, RDLFE («[c]uando la garantía que, en su caso, hubieran constituido los prestadores de servicios de certificación no sea suficiente para satisfacer la indemnización debida, responderán de la deuda, con todos sus bienes presentes y futuros». Por lo demás, el artículo 22.2, 22.3 y 22.4 LFE no tiene equivalente en el RDLFE. Asimismo, el artículo 22.5 LFE se corresponde con el artículo 14.4 RDLFE. Por último, el artículo 14.2 RDLFE no tiene equivalente en el artículo 22 LFE, sí con el artículo 23.1.f) LFE.

(41) El artículo 23.1.f) LFE se corresponde con el artículo 14.2 RDLFE. Además, ninguno de los apartados del artículo 23 LFE, salvo el artículo 23.1.f) RDLFE, tienen su correspondiente, ni en la DFE ni en el RDLFE.

(42) La LFE modifica el concepto de certificación de PSSIic. Se recoge el concepto de *acreditación* de PSSIic contenido en la DFE, si bien la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la LI. El artículo 26 LFE clarifica los conceptos y no establece distinción alguna entre certificación de la actividad del PSSIic o certificación del producto de firma electrónica que emplee dicho PSSIic. Para concluir, el artículo 26.4 LFE introduce una importante novedad, como es la de afirmar que esta certificación voluntaria de los PSSIic no será necesaria para reconocer eficacia jurídica a una firma electrónica, si bien es cierto que favorece la seguridad y la confianza en la actividad de prestación de SSIic.

(43) Se recoge el concepto de *acreditación* de PSSIic contenido en la DFE, si bien la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la LI.

(44) El artículo 25.3, *ab initio*, LFE, en su comparativa con la DFE y al RDLFE, añade que los dispositivos de verificación de firma electrónica garantizarán, «siempre que sea técnicamente posible», que el proceso de verificación de una firma electrónica satisfaga, al menos, los requisitos en él enumerados; ello deja abierta la posibilidad a su incumplimiento argumentando que no fue técnicamente posible (no así la DFE ni el RDLFE). Este mismo artículo 25.3, *ab initio*, LFE elimina la anterior mención

(entiendo, errónea) del RDLFE (no así la DFE), que reducía los requisitos que tenían que cumplir los dispositivos de verificación de firma electrónica sólo a la firma electrónica avanzada (bien es cierto que en el RDLFE no existía aún el término *firma electrónica reconocida*, que se crea con la LFE, pero tampoco especificaba si se refería a la firma electrónica avanzada equivalente a la posterior firma electrónica reconocida (aquella basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma electrónica) o a la actual firma electrónica avanzada. El artículo 25.3 LFE introduce un apartado a) no contemplado hasta ahora, ni en la DFE ni en el RDLFE. Además, se incorpora un artículo 25.4 LFE que no existía ni en la DFE ni en el RDLFE. Por último, se elimina la previsión contenida en el artículo 22.2 RDLFE.

(45) Dado que rige el principio de no sujeción a autorización previa, se refuerzan las capacidades de supervisión y control.

(46) La LFE, a diferencia del RDLFE (la DFE no regula este aspecto), no sólo regula el deber de información y de colaboración de los PSSIic, sino también de la entidad independiente de acreditación y de los organismos de certificación. Además, la LFE incorpora los apartados 2 y 3 al artículo 30, que no estaban recogidos en el RDLFE (tampoco en la DFE que, como decimos, no regula este aspecto).

(47) ¿Por qué la LFE no contempla una posible graduación de la cuantía de las sanciones, al estilo del artículo 39 bis LSSICE?

(48) La D. F. 1ª LFE introduce como fundamento constitucional, a diferencia del RDLFE, el recogido en el artículo 149.1.29ª LFE. Los demás coinciden en ambas leyes (artículo 149.1.8ª, 18ª y 21ª LFE).

(49) Regulando también el ámbito de aplicación, se limita a establecer la transposición de la DFE, de modo similar a lo que hace la LFE en la Exposición de Motivos.

(50) El artículo 2.1.a) DLDFE habla de la firma electrónica como medio de autenticación, al igual que el artículo 2.1) DFE y a diferencia del artículo 3.1 LFE.

(51) Se remite a lo que los anexos I y II DFE.

(52) Este apartado del artículo 6 DLDFE no encuentra equivalente a nivel europeo ni interno español.

(53) A los efectos que aquí interesan, artículo 2.3 de la norma (Capítulo II, comprensivo de las Secciones I y II –artículos 20 a 37–). La rúbrica del Capítulo II fue modificada y sustituida por el apartado primero del artículo 17 y por el apartado primero del artículo 26, ambos del PDLMICAD.

(54) Los artículos 20 y 23, a diferencia de su equivalente español y europeo, introducen reglas respecto de la transmisión, conservación, duplicación, reproducción y validación temporal de los documentos informáticos (artículo 20), así como sobre la copia de los mismos (artículo 23). El artículo 24, al igual que el artículo 1.s), del DL 82/2005 define y establece reglas, respectivamente, en relación con la firma digital, no mencionada ni regulada a nivel europeo ni interno español. El artículo 25 DL 82/2005 regula la firma autenticada por notario o por otro oficial público autorizado, a diferencia de la normativa europea e interna española.

(55) No se incluyen en este apartado las obligaciones contenidas en el artículo 20.b), e) y f), que sería su equivalente en el ordenamiento jurídico español.

Anexo XV. El Reglamento sobre identificación electrónica y servicios de confianza para las transacciones electrónicas y su transposición al ordenamiento jurídico interno, español e italiano

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Objeto | 1 | 1.1 (24) | - | 1 | 2 | En el apartado primero del artículo 2, después de la palabra *modalidad más apropiada*, se introducen las siguientes *y en el modo más apropiado a la satisfacción de los intereses de los usuarios*, todo ello merced a la letra a) del apartado primero del artículo 2 SDLMICAD / El apartado segundo del artículo 2 e sustituido por una nueva redacción, merced a la letra b) del apartado primero del artículo 2 SDLMICAD/ Los apartados 5 y 6 del artículo 2 son sustituidos por una nueva redacción, merced a la letra c) del apartado primero del artículo 2 SDLMICAD |
| Ámbito de aplicación | 2 | 1.2, 2.1, 2.3, 2.4 y 2.5 (25) | - | 2 (37) | | |
| Definiciones | 3.1) | - | - | - | - | - |
| | 3.2) | - | - | - | - | - |
| | 3.3) | - | - | - | - | - |
| | 3.4) | - | - | - | - | - |
| | 3.5) | - | - | - | - | - |
| | 3.6) | - | - | - | - | - |
| | 3.7) | - | - | - | - | - |
| | 3.8) | - | - | - | - | - |
| | 3.9) | 6.2 (26) | - | - | 1.aa) | - |
| | 3.10) | 3.1 | - | - | - | - |
| | 3.11) y 26 | 3.2 | Se modifica el artículo 3.2 LFE por la D. F. 4.1 LMSO | - | - | - |
| | 3.12) (1) | 3.3 | - | - | - | - |
| | 3.13) | 24.1 (27) | - | - | - | - |
| | 3.14) (2) | 6.1 | - | - | - | - |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| | 3.15) y anexo I (3) | 11.1 y 11.2 | - | - | 33 | - |
| | 3.16) | - | - | - | - | - |
| | 3.17) | - | - | - | - | - |
| | 3.18) | - | - | - | - | - |
| | 3.19) (4) | 2.2 | - | - | - | - |
| | 3.20) | - | - | - | - | - |
| | 3.21) | 28 | - | - | - | - |
| | 3.22) | 24.2 | - | - | - | - |
| | 3.23) y anexo II | 24.3 | - | - | 35 | Al artículo 35 le son aplicables las siguientes modificaciones: el título es sustituido por el de *dispositivos seguros y procedimientos para la generación de la firma cualificada*, merced a la letra a) del apartado primero del artículo 30 SDLMICAD; después del apartado 1 se incorpora un apartado 1 bis, merced a la letra b) del apartado primero del artículo 30 SDLMICAD; en el apartado 5, después de las palabras *de una firma* se incorpora la palabra *electrónica*, después de la palabra *cualificada* se incorporan las palabras *o de un sello electrónico* y, por último, las palabras *del anexo III de la Directiva 1999/93/CE* son sustituidas por las palabras *del anexo II del Reglamento eIDAS*, merced a la letra c) del apartado primero del artículo 30 SDLMICAD, y, por último, el apartado 6 es reemplazado por una nueva redacción, merced a la letra d) del apartado primero del artículo 30 SDLMICAD |
| | 3.24) | - | - | - | - | - |
| | 3.25) | - | - | - | - | - |
| | 3.26) | - | - | - | - | - |
| | 3.27) | - | - | - | 1.v bis) | - |
| | 3.28) | - | - | - | - | - |
| | 3.29) | - | - | - | - | - |
| | 3.30) y anexo III | - | - | - | - | - |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| | 3.31) | - | - | - | - | - |
| | 3.32) | - | - | - | - | - |
| | 3.33) | - | - | - | - | - |
| | 3.34) y 42 | - | - | - | - | - |
| | 3.35) | 3.5 | Se modifica el artículo 3.5 LFE por los artículos 5.1 y 5.2 LMISI | - | 1.p) | Letra 1.p) sustituida por la redacción proporcionada por la letra d) del apartado primero del artículo 1 SDLMICAD |
| | 3.36) | - | - | - | - | - |
| | 3.37) y 44 | - | - | - | - | - |
| | 3.38) | - | - | - | - | - |
| | 3.39) y anexo IV | - | - | - | 33 | - |
| | 3.40) | - | - | - | - | - |
| | 3.41) | - | - | - | - | - |
| | - | - | - | - | 1.oa) | Letra 1.oa) incorporada, antes de la letra 1.a), por la letra a) del apartado primero del artículo 1 SDLMICAD |
| | - | - | - | - | 1.d) | - |
| | - | - | - | - | 1.i.bis) | - |
| | - | - | - | - | 1.i.ter) | - |
| | - | - | - | - | 1.i.quater) | - |
| | - | - | - | - | 1.5.quinquies) | - |
| | - | - | - | - | 1.i.sexies) | Letra 1.i sexies) incorporada, después de la letra 1.i quinquis), por la letra b) del apartado primero del artículo 1 SDLMICAD |
| | - | - | - | - | 1.n bis) | - |
| | - | - | - | - | 1.n ter) | Letra 1.n ter) incorporada, después de la letra 1.n bis), por la letra c) del apartado primero del artículo 1 SDLMICAD |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| | - | - | - | - | 1.p bis) | - |
| | - | - | - | - | 1.s) | En la letra 1.s), la palabra *electrónica avanzada* es sustituida por la palabra *cualificada*, y las palabras *certificado cualificado y* son suprimidas, todo ello merced a la letra e) del apartado primero del artículo 1 SDLMICAD |
| | - | - | - | - | 1.u bis) | - |
| | - | - | - | - | 1.u quater) | Letra 1.u quater) incorporada, después de la letra 1.u ter) por la letra f) del apartado primero del artículo 1 SDLMICAD |
| | - | - | - | - | 1.v) | - |
| | - | - | - | - | 1.cc) | Letra 1.cc) incorporada, después de la letra 1.bb), por la letra g) del apartado primero del artículo 1 SDLMICAD |
| | - | - | - | - | 1.dd) | Letra 1.cc) incorporada, después de la letra 1.bb), por la letra g) del apartado primero del artículo 1 SDLMICAD |
| | - | - | - | - | 1.ee) | Letra 1.cc) incorporada, después de la letra 1.bb), por la letra g) del artículo 1 SDLMICAD |
| | - | - | - | - | 1 bis | Letra 1 bis incorporada, después del apartado primero, por el apartado segundo del artículo 1 SDLMICAD |
| | - | - | - | - | 1 ter | Letra 1 ter incorporada, después del apartado primero, por el apartado segundo del artículo 1 SDLMICAD |
| Principio del mercado interior | 4 (5) | 5 (28) | - | - | - | - |
| Tratamiento y protección de los datos | 5 | 17 | - | 10 (38) | 33 | - |
| Reconocimiento mutuo | 6 | - | - | - | - | - |
| Condiciones para la notificación de los sistemas de identificación electrónica | 7 | 3.11 | Se añade el artículo 3.11, con efectos de 2 de octubre de 2016, por la D. F. 2 LPACAP | D. A. 2ª | - | - |
| Niveles de seguridad de los sistemas de identificación electrónica | 8 (6) | | | | - | - |
| Notificación de los sistemas de identificación electrónica | 9 (7) | | | | - | - |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Violación de la seguridad de los sistemas de identificación electrónica | 10 | | | | - | - |
| Responsabilidad del Estado miembro notificador de los sistemas de identificación electrónica | 11 | | | | - | - |
| Cooperación e interoperabilidad de los sistemas de identificación electrónica | 12 (8) | | | | - | - |
| Responsabilidad y carga de la prueba de los PSSIisc | 13.1 (9) | 22 | - | 13 | 30.1 | Al artículo 30 se incorporan las siguientes modificaciones: el título es sustituido por el de *responsabilidad de los prestadores de servicios de confianza cualificados, de los gestores de correo electrónico certificado, de los gestores de la identidad digital y de los conservadores*, merced a la letra a) del apartado primero del artículo 26 SDLMICAD; el apartado 1 es sustituido por una nueva redacción, merced a la letra b) del apartado primero del artículo 26 SDLMICAD, y, por último, el apartado 2 es suprimido, merced a la letra c) del apartado primero del artículo 26 SDLMICAD |
| Limitaciones a la responsabilidad de los PSSIisc | 13.2 | 23 | Se modifica el artículo 23.5 por el artículo 5.4 LMISI / Se modifican los apartados 1.c) y d) del artículo 23 por la D. F. 4.8 LMSO | 14 | 30.3 | |
| Aspectos internacionales | 14 (10) | 14 | - | - | - | - |
| Accesibilidad para personas con discapacidad | 15 | D. A. 9ª | - | - | - | - |
| Infracciones | - | 31 (29) | Se modifica el apartado 4 del artículo 31 por el artículo 5.5 LMISI | 21 | - | - |
| Sanciones | 16 | 32 (30) | - | 22.1 y 22.3 (39) | 32 bis | Al artículo 32 bis se incorporan las siguientes modificaciones: el título es reemplazado por el de *sanciones para los prestadores de servicios de confianza cualificados, para los gestores de correo electrónico certificado, para los gestores de la identidad digital y para los conservadores*, merced a la letra a) del apartado primero del artículo 28 SDLMICAD; el apartado 1 es sustituido por una nueva redacción, merced a la letra b) del apartado primero del artículo 28 SDLMICAD; después del apartado 1 se incorpora un apartado 32.1 bis, merced a la letra c) del apartado primero del artículo 28 SDLMICAD; en el apartado 2, las palabras *en el sistema* son reemplazadas por las palabras *en los sistemas de correo electrónico certificado* y las palabras *el certificador cualificado o* son derogadas, merced a la letra d) del apartado primero del artículo 28 SDLMICAD; en el apartado 3, después de las palabras *apartado 1* se incorporan las palabras *1 bis*, merced a la letra e) del apartado primero del artículo 28 SDLMICAD, y, por último, el apartado 4 es suprimido, merced a la letra f) del apartado primero del artículo 28 SDLMICAD |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Graduación de la cuantía de las sanciones | - | 33 (31) | - | 22.2 (40) | - | - |
| Medidas provisionales | - | 34 (32) | - | - | - | - |
| Multa coercitiva | - | 35 (33) | - | - | - | - |
| Competencia y procedimiento sancionador | - | 36 (34) | - | 23 (41) | - | - |
| Organismo de supervisión | 17 | 29 | - | 17 y 18 | - | - |
| Asistencia mutua de los organismos de supervisión | 18 | - | - | | - | - |
| Requisitos de seguridad aplicables a los PSSIisc | 19 | - | - | 16 | - | - |
| Supervisión de los PSSIisc cualificados | 20 | 26 | - | 17 | - | - |
| Inicio de un SSIisc cualificado | 21 | - | - | - | 29 | Al artículo 29 se incorporan las siguientes modificaciones: el título es sustituido por el de *cualificación y acreditación*, merced a la letra a) del apartado primero del artículo 25 SDLMICAD; el apartado 1 es reemplazado por una nueva redacción, merced a la letra b) del apartado primero del artículo 25 SDLMICAD; el apartado 2 es sustituido por una nueva redacción, merced a la letra c) del apartado primero del artículo 25 SDLMICAD; el apartado 3 es reemplazado por una nueva redacción, merced a la letra d) del apartado primero del artículo 25 SDLMICAD; en el apartado 4, la palabra *acreditación* es sustituida por las palabras *cualificación o de acreditación*, merced a la letra e) del apartado primero del artículo 25 SDLMICAD; en el apartado 6, después de la palabra *lista* se incorporan las palabras *de confianza*, merced a la letra f) del apartado primero del artículo 25 SDLMICAD, y, por último, los apartados 7 y 8 son suprimidos, merced a la letra g) del apartado primero del artículo 25 SDLMICAD |
| Listas de confianza de PSSIisc | 22 (11) | - | - | 19 | - | - |
| Etiqueta de confianza «UE» para servicios de confianza cualificados | 23 (12) | - | | - | - | - |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Requisitos para los PSSIisc | 24 | 12, 13, 17, 18, 19, 20 y 21 | Se modifica el apartado c) del artículo 12 por la D. F. 4.4 LMSO / Se modifican los apartados 2 y 3 del artículo 13 por el artículo 5.3 LMISI / Se modifican el apartado a) y el b).1 del artículo 18 por la D. F. 4.5 y 4.6 LMSO / Se modifica el apartado 1.e) del artículo 20 por la D. F. 4.7 LMSO | 7, 11 y 12 (42) | 32.2, 32.3, 32.4, 32.5 y 37 (48) | A estos apartados del artículo 32 le son aplicables las siguientes modificaciones: la palabra *certificador* es sustituida, en todos aquellos apartados en que se emplea, por las palabras *prestadores de servicios de firma electrónica cualificada*, merced a la letra c) del apartado primero del artículo 27 SDLMICAD; en el apartado 3, la palabra *asimismo*, es sustituida por las palabras *de todas maneras*, merced a la letra d) del apartado primero del artículo 27 SDLMICAD; en el mismo apartado 3, letra g), después de las palabras *alteración del dispositivo de firma*, se incorporan las palabras *o de los instrumentos de autenticación informática para la utilización del dispositivo de firma*, merced a la letra e) del apartado primero del artículo 27 SDLMICAD, y, por último, en el apartado 5, las palabras *recoge los datos personales sólo directamente de la persona a la cual se refieren o previamente a su consentimiento expreso* son reemplazadas por las palabras *recoge los datos personales directamente de la persona a la cual se refieren o, previamente a su consentimiento expreso, a través dle tercero*, merced a la letra f) del apartado primero del artículo 27 SDLMICAD / Al artículo 37 le son aplicables las siguientes modificaciones: en el apartado 1, las palabras *el certificador cualificado o acreditado* son sustituidas por las palabras *el prestador de servicios de confianza cualificado*, merced a la letra a) del apartado primero del artículo 31 SDLMICAD; en el apartado 2, la palabra *certificador* es reemplazada por la palabra *prestador* y, después, la palabra *certificador* es sustituida por las palabras *prestador de servicios de confianza cualificado*, merced a la letra b) del apartado primero del artículo 31 SDLMICAD; en el apartado 3, la palabra *certificador* es sustituida por la palabra *prestador*, merced a la letra c) del apartado primero del artículo 31 SDLMICAD; en el apartado 4, las palabras *certificador acreditado* son sustituidas por las palabras *prestador al que se refiere el apartado 1*, merced a la letra d) del apartado primero del artículo 31 SDLMICAD; en el apartado 4 bis, las palabras *certificador cualificado* son sustituidas por las palabras *prestador al que se refiere el apartado 1* y las palabras *un certificador* son reemplazadas por las palabras *un prestador de servicios de confianza cualificado*, merced a la letra e) del apartado primero del artículo 31 SDLMICAD, y, por último, después del apartado 4 bis, se incluye un apartado 4 ter, merced a la letra f) del apartado primero del artículo 31 SDLMICAD |
| SSIisc no cualificados | - | - | - | 15 | - | - |
| Efectos jurídicos de las firmas electrónicas | 25 (13) | 3.4, 3.9 y 3.10 | - | - | - | - |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Firmas electrónicas en servicios públicos | 27 (14) | 3.11 y 4 | - | - | 22 y 34 | El apartado 6 del artículo 22 es suprimido por el apartado primero del artículo 19 SDLMICAD / Al artículo 34 le son aplicables las siguientes modificaciones: el título es sustituido por el de *nombres particulares para las Administraciones públicas*, merced a la letra a) del apartado primero del artículo 29 SDLMICAD; en el apartado 1, la letra a), la palabra *acreditarse* es reemplazada por la palabra *cualificarse* y el último período es suprimido, merced a la letra b) del apartado primero del artículo 29 SDLMICAD, y, por último, los apartados 3, 4 y 5 son derogados, merced a la letra c) del apartado primero del artículo 29 SDLMICAD |
| Certificados electrónicos de personas jurídicas | - (15) | 7 | - | - | - | - |
| Certificados cualificados de firma electrónica | 28 y anexo I | 8, 9, 10 y 11 | Se modifica el apartado 2 del artículo 8 por la D. F. 6ª LGT | 4, 5 y 6 | 28 y 36 | Al artículo 28 se incorporan las siguientes modificaciones: el título es sustituido por el de *certificadores de firma electrónica cualificada*, merced a la letra a) del apartado primero del artículo 24 SDLMICAD; el apartado 1 es suprimido, merced a la letra b) del apartado primero del artículo 24 SDLMICAD; el apartado 2 es reemplazado por una nueva redacción, merced a la letra c) del apartado primero del artículo 24 SDLMICAD, y, en el apartado 3, las palabras *certificado cualificado* son sustituidas por las palabras *certificado de firma electrónica cualificada* y, después de las palabras *si procede*, se incorporan las palabras *y no excesivos con respecto*, merced a la letra d) del apartado primero del artículo 24 SDLMICAD |
| DNIe | - | 15 | - | 8 | 1.c) y 66 | Al artículo 66 le son aplicables las siguientes modificaciones: en el apartado 8, después de las palabras *modalidad electrónica* se incorporan las palabras *de acuerdo con las reglas técnicas a que hace referencia el artículo 71*, merced a la letra a) del apartado primero del artículo 52 SDLMICAD; asimismo, el apartado 8 bis es derogado, merced a la letra b) del apartado primero del artículo 52 SDLMICAD |
| Requisitos y características del DNIe | - | 16 | - | 9 (43) | | |
| Requisitos de los dispositivos cualificados de creación de firmas electrónicas | 29 y anexo II | 24 | - | - | - | - |
| Certificación de los dispositivos cualificados de creación de firmas electrónicas | 30 (16) | 27 | - | - | 35 | Al artículo 35 le son aplicables las siguientes modificaciones: el título es sustituido por el de dispositivos seguros y procedimientos para la generación de la firma cualificada, merced a la letra a) del apartado primero del artículo 30 SDLMICAD; después del apartado 1 se incorpora un apartado 1 bis, merced a la letra b) del apartado primero del artículo 30 SDLMICAD; en el apartado 5, después de las palabras de una firma se incorpora la palabra electrónica, después de la palabra cualificada se incorporan las palabras *o de un sello electrónico* y, por último, las *palabras del anexo III de la Directiva 1999/93/CE* son sustituidas por las *palabras del anexo II del Reglamento eIDAS*, merced a la letra c) del apartado primero del artículo 30 SDLMICAD, y, |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| | | | | | | por último, el apartado 6 es reemplazado por una nueva redacción, merced a la letra d) del apartado primero del artículo 30 SDLMICAD |
| Publicación de una lista de dispositivos cualificados de creación de firmas electrónicas certificados | 31 | - | - | - | - | - |
| Requisitos de la validación de las firmas electrónicas cualificadas | 32 (17) | 25 | - | - | 33 | - |
| Servicio de validación cualificado de firmas electrónicas cualificadas | 33 (17) | | - | - | - | - |
| Servicio cualificado de conservación de firmas electrónicas cualificadas | 34 | - | - | - | - | - |
| Firma digital | - | - | - | - | 24 | Al artículo 24 se incorporan las siguientes modificaciones: al apartado 4, las palabras *establecidas en los términos del artículo 71* son sustituidas por las palabras *con arreglo al artículo 71*, merced a la letra a) del apartado primero del artículo 22 SDLMICAD; además, después del apartado 4, son incorporados los apartados 4 bis y 4 ter, merced a la letra b) del apartado primero del artículo 22 SDLMICAD |
| Firma autenticada | - | - | - | - | 25 | Al artículo 25 se incorporan las siguientes modificaciones: al apartado 1, después de las palabras *tipo de firma*, se incorpora la palabra *electrónica*, merced a la letra a) del apartado primero del artículo 25 SDLMICAD; además, en el apartado 4, la palabra *apartado 5* es suprimida, merced a la letra b) del apartado primero del artículo 25 SDLMICAD |
| Obligaciones del titular del certificado de firma electrónica | - | - | - | - | 32.1 | Al artículo 32 1 le son aplicables las siguientes modificaciones: el título es sustituido por el de *obligaciones del titular y del prestador de servicios de firma electrónica cualificada*, merced a la letra a) del apartado primero del artículo 27 SDLMICAD; además, en el apartado 1, después de las palabras *custodia del dispositivo de firma*, se incorporan las palabras *o de los instrumentos de autenticación informática para la utilización del dispositivo de firma de forma remota* |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Efectos jurídicos del sello electrónico | 35 (18) | - | - | - | - | - |
| Requisitos para los sellos electrónicos avanzados | 36 (19) | - | - | - | - | - |
| Sellos electrónicos en servicios públicos | 37 (20) | - | - | - | - | - |
| Certificados cualificados de sello electrónico | 38 (21) | - | - | - | - | - |
| Requisitos de los dispositivos cualificados de creación de sellos electrónicos | 39 (22) | . | . | - | - | - |
| Validación y conservación de sellos electrónicos cualificados | 40 (23) | - | - | - | - | - |
| Efectos jurídicos de los sellos de tiempo electrónicos | 41 | - | - | - | - | - |
| Requisitos para los sellos de tiempo electrónicos cualificados | 42 | - | - | - | - | - |
| Efectos jurídicos de los servicios de entrega electrónica certificada | 43 | - | - | - | - | - |
| Requisitos para los servicios de entrega electrónica certificada cualificados | 44 | - | - | - | - | - |
| Requisitos de los certificados cualificados de autenticación de sitios web | 45 | - | - | - | - | - |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Efectos jurídicos de los documentos electrónicos | 46 | 3.6, 3.7 y 3.8 | Se modifica el artículo 3.8 por los artículos 5.1 y 5.2 LMISI | 3 (44) | 20, 21, 23, 23 bis, 23 ter y 23 quater | Al artículo 20 se incorporan una serie de modificaciones: la rúbrica del artículo es sustituida por la de *validez y eficacia probatoria de los documentos informáticos*, merced a la letra a) del apartado primero del artículo 17 SDLMICAD; el apartado 1 es suprimido, merced a la letra b) del apartado primero del artículo 17 SDLMICAD; la letra 1 bis es sustituida por una nueva redacción, merced al apartado c) del apartado primero del artículo 17 SDLMICAD, y , en el apartado 3, las palabras *temporal* y *avanzada*, son suprimidas, merced a la letra d) del apartado primero del artículo 17 SDLMICAD / Al artículo 21 se incorporan una serie de modificaciones: al apartado 1, después de las palabras *firma electrónica*, se incorporan las palabras *satisfaga el requisito de la forma escrita y*, merced a la letra a) del apartado primero del artículo 18 SDLMICAD; el apartado 2 es sustituido por una nueva redacción, merced a la letra b) del apartado primero del artículo 18 SDLMICAD; en el apartado 2 bis, las palabras *salvo cuanto esté previsto por el artículo 25* son sustituidas por las palabras *salvo en el caso de suscripción autenticada* y las palabras *satisfagan de todos modos el requisito de la forma escrita si suscriben con firma electrónica avanzada, cualificada o digital* son sustituidas por las palabras *redactados sobre documento informático o formados a través de procedimientos informáticos son suscritos, bajo pena de nulidad, con firma electrónica avanzada, cualificada o digital*, todo ello merced a la letra c) del apartado primero del artículo 18 SDLMICAD; después del apartado 2 bis se incorpora un apartado 2 ter, merced a la letra d) del apartado primero del artículo 18 SDLMICAD, y, por último, los apartados 3 y 4 son suprimidos, merced a la letra e) del apartado primero del artículo 18 SDLMICAD / Al artículo 23, después del apartado 2, se incorpora un apartado 2 bis, merced al apartado primero del artículo 20 SDLMICAD / Al artículo 23 ter se incorporan las siguientes modificaciones: el apartado 4 es sustituido por una nueva redacción, merced a la letra a) del apartado primero del artículo 21 SDLMICAD, mientras que los apartados 2 y 5 son suprimidos, merced a la letra b) del apartado primero del artículo 21 SDLMICAD |
| Deber de información y colaboración | - | 30 | - | 20 (45) | - | - |
| Ejercicio de la delegación | 47 | - | - | - | - | - |
| Procedimiento de comité | 48 | - | - | - | - | - |
| Revisión | 49 | - | - | - | - | - |
| Fe pública y uso de firma electrónica | - | D. A. 1ª | - | D. A. 1ª | - | - |

| Concepto | UE | España | | | Italia | |
|---|---|---|---|---|---|---|
| | RIE-SCTE | LFE | | ALSEC | CAD | |
| | Artículos | Artículos | Modificaciones | Artículos | Artículos | Modificaciones |
| Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica | - | D. A. 2ª | - | - | - | - |
| Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias | - | D. A. 3ª | - | - | - | - |
| PSSIisc por la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda | - | D. A. 4ª | - | - | - | - |
| Modificación del artículo 81 PLMFAOS | - | D. A. 5ª | - | - | - | - |
| Régimen jurídico del DNIe | - | D. A. 6ª | - | - | - | - |
| Emisión de facturas por vía electrónica | - | D. A. 7ª | - | - | - | - |
| Modificación de la LSSICE | - | D. A. 8ª | - | - | - | - |
| Modificación de la LECiv | - | D. A. 10ª | - | - | - | - |
| Modificación de la LMISI | - | - | - | D. F. 1ª | - | - |
| Resolución de conflictos | - | D. A. 11ª (35) | Se añade la D. A. 11ª por el artículo 5.6 LMISI | - | - | - |
| Derogación normativa | 50 | D. D. Única | - | D. D. Única | 91 | - |
| Medidas transitorias | 51 | D. T. 1ª y D. T. 2ª (36) | - | D. T. Única (46) | - | - |
| Fundamento constitucional | - | D. F. 1ª | - | D. F. 2ª (47) | - | - |
| Desarrollo reglamentario | - | D. F. 2ª | - | D. F: 3ª | - | - |
| Entrada en vigor | 52 | D. F. 3ª | - | - | | - |

*Anexo XV. El Reglamento sobre identificación electrónica y servicios de confianza para las transacciones electrónicas y su transposición al ordenamiento jurídico interno, español e italiano. Fuente: elaboración propia*

(1) Con el RIE-SCTE, se sustituyen los términos *firma electrónica reconocida*, *dispositivo seguro de creación de firma electrónica* y *certificado reconocido de firma electrónica* por los de *firma electrónica cualificada*, *dispositivo cualificado de creación de firma electrónica* y *certificado cualificado de firma electrónica*, respectivamente.

(2) Con el RIE-SCTE, se sustituyen los términos *certificado electrónico* y *datos de verificación de firma electrónica* por los de *certificado de firma electrónica* (al incorporarse nuevas modalidades de certificados electrónicos) y *datos de validación de firma electrónica*, respectivamente. Además, mientras la LFE establecía que el certificado de firma electrónica servía para confirmar la identidad general de la persona, el RIE-SCTE establece, dentro de esa identidad, un mínimo que el certificado de firma electrónica debe confirmar, como es el nombre o el seudónimo de la persona certificada.

(3) En línea con la nota (1), con el RIE-SCTE, se sustituye el término *certificado electrónico reconocido* por el de *certificado cualificado de firma electrónica* (al incorporarse nuevas modalidades de certificados electrónicos).

(4) Con el RIE-SCTE, se sustituye el término *prestador de servicios de certificación* por el de *prestador de servicios de confianza* (al comprender actividades más amplias que la sola certificación).

(5) No se habla de la no sujeción a autorización previa, manteniéndose el principio de libre prestación de SSIisc.

(6) Al amparo del artículo 8.3 RIE-SCTE, se publica el REFEPTMNSMIE.

(7) Al amparo del artículo 9.5 RIE-SCTE, se publica la DECFPN.

(8) Al amparo del artículo 12.7 RIE-SCTE, se publica la DEMPCEMMIE. Al amparo del artículo 12.8 RIE-SCTE, se publica el REMI.

(9) A diferencia de la LFE, el RIE-SCTE distingue entre *PSSIisc no cualificados*, donde la carga de la prueba recaerá sobre la persona, física o jurídica, que alegue los perjuicios, y *PSSIisc cualificados*, a los que se les presumirá intencionalidad o negligencia, salvo cuando demuestren que los perjuicios se produjeron sin intención ni negligencia por su parte.

(10) La LFE exige mayores requisitos a la hora de otorgar esta equivalencia, ya que exige que el PSSIisc del tercer país haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del EEE y que el certificado (concreto SSIisc) esté garantizado por un PSSIisc establecido en el EEE que cumpla los

requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos. Además, como vemos, la LFE establece esta equivalencia internacional sólo para un concreto SSIisc, como es el certificado electrónico, mientras que el RIE-SCTE la permite para cualquier SSIisc.

(11) Al amparo del artículo 22.5 RIE-SCTE, se publica la DEETFLC.

(12) Al amparo del artículo 23.3 RIE-SCTE, se publica el REERFECUESCC.

(13) El artículo 25 RIE-SCTE introduce una importante previsión, contenida en su apartado tercero y último, cual es aquella que establece que la firma electrónica cualificada emitida en un Estado miembro será reconocida como firma electrónica cualificada en todos los demás Estados miembros.

(14) Al amparo del artículo 27.5 RIE-SCTE, se publica la DEEFFEASEA.

(15) El nuevo paradigma instaurado por el RIE-SCTE implica que únicamente las personas físicas están capacitadas para firmar electrónicamente, por lo que no prevé la emisión de certificados de firma electrónica a favor de personas jurídicas o entidades sin personalidad jurídica. A éstas se reservan los sellos electrónicos, que permiten garantizar la autenticidad e integridad de sus documentos, tales como facturas electrónicas y activos digitales, sin perjuicio de poder actuar por medio de los certificados de firma de persona física con atributo de representante.

(16) Al amparo del artículo 30.3 (y del artículo 39.2) RIE-SCTE, se publica la DENESDCCFS.

(17) En la RIE-SCTE no consta la alusión a los dispositivos de verificación (validación) de firma electrónica, de los que sí habla explícitamente la LFE.

(18) Equivalente con el artículo 25 RIE-SCTE.

(19) Equivalente con el artículo 26 RIE-SCTE.

(20) Equivalencia con el artículo 27 RIE-SCTE. Al amparo del artículo 37.5 RIE-SCTE, se publica la DEEFFEASEA.

(21) Equivalencia con el artículo 28 RIE-SCTE.

(22) Equivalencia con los artículos 29, 30 y 31 RIE-SCTE.

(23) Equivalente a los artículos 32, 33 y 34 RIE-SCTE.

(24) Controversia en cuanto a la determinación del ámbito de aplicación en su comparación con la LSSICE, también aplicable en estos casos.

(25) Coincidencia exacta del artículo 2.3 LFE con el artículo 2.1.2º LSSICE. Coincidencia exacta del artículo 2.4 LFE con el artículo 2.2.2º LSSICE. Coincidencia exacta del artículo 2.5 LFE con el artículo 2.3 LSSICE.

(26) La LFE, a diferencia del RIE-SCTE, aclara que el firmante puede actuar en nombre propio o en nombre de una persona, física o jurídica, a la que representa. El RIE-SCTE, al hablar de identificación electrónica, no contempla, sin embargo, el supuesto de persona física que representa a otra persona física.

(27) La LFE, en su definición, añade un supuesto de datos de creación de firma electrónica, como serían los códigos o claves criptográficas privadas; el RIE-SCTE, no.

(28) Concordancia con el artículo 7 LSSICE.

(29) Dado que los PSSIisc están, a mi juicio, subsumidos en la categoría más genérica de PSSIi (dentro, a su vez, de la noción más amplia de PSSI), este artículo debería complementarse con cuanto establece el artículo 38 LSSICE.

(30) Dado que los PSSIisc están, a mi juicio, subsumidos en la categoría más genérica de PSSIi (dentro, a su vez, de la noción más amplia de PSSI), este artículo debería complementarse con cuanto establece el artículo 39 LSSICE.

(31) Dado que los PSSIisc están, a mi juicio, subsumidos en la categoría más genérica de PSSIi (dentro, a su vez, de la noción más amplia de PSSI), este artículo debería complementarse con cuanto establece el artículo 40 LSSICE.

(32) Dado que los PSSIisc están, a mi juicio, subsumidos en la categoría más genérica de PSSIi (dentro, a su vez, de la noción más amplia de PSSI), este artículo debería complementarse con cuanto establece el artículo 41 LSSICE.

(33) Dado que los PSSIisc están, a mi juicio, subsumidos en la categoría más genérica de PSSIi (dentro, a su vez, de la noción más amplia de PSSI), este artículo debería complementarse con cuanto establece el artículo 42 LSSICE.

(34) Dado que los PSSIisc están, a mi juicio, subsumidos en la categoría más genérica de PSSIi (dentro, a su vez, de la noción más amplia de PSSI), este artículo debería complementarse con cuanto establece el artículo 43 LSSICE.

(35) Dado que los PSSIisc están, a mi juicio, subsumidos en la categoría más genérica de PSSIi (dentro, a su vez, de la noción más amplia de PSSI), este artículo debería complementarse con cuanto establece el artículo 32 y la D. A. 3ª LSSICE.

(36) La D. T. 1ª LFE es equivalente, en el ordenamiento jurídico interno español, al artículo 51.2 RIE-SCTE. Lo mismo sucede con la D. T. 2ª LFE, equivalente, en nuestro ordenamiento jurídico interno, al artículo 51.3 y 51.4 RIE-SCTE.

(37) Mantiene exactamente la misma redacción que la LFE, con todas las connotaciones que, en consecuencia, se han de seguir manteniendo en cuanto a la relación de la normativa en materia de firma electrónica con los artículos 2 a 5 LSSICE.

(38) El artículo 10 ALSEC se corresponde con los apartados 3 y 4 del artículo 17 LFE, no incluyéndose en él cuanto se dispone en los apartados 1 y 2 de dicho artículo.

(39) Por lo que respecta al artículo 22.1 ALSEC, cambia el importe de las posibles sanciones: para las infracciones muy graves, ya no es de 150.001,00€ hasta 600.000,00€, sino de 150.001,00€ hasta 300.000,00€; para las infracciones graves, ya no es de 30.001,00€ hasta 150.000,00€, sino de 50.001€ hasta 150.000,00€, y, para las infracciones leves, ya no es hasta 30.000,00€, sino de 5.000,00€ hasta 50.00,00€. Con ello, se produce una diferencia sustancial con respecto a las sanciones previstas en la LSSICE, cuyas consecuencias habrá que analizar a la vista de la aplicación conjunta de ambas normas. Por último, el artículo 32.1.a).2º LFE contempla una importante previsión que desaparece en el artículo 22.1.a) ALSEC, relativa a la posible sanción de prohibición en España durante un plazo máximo de dos años como consecuencia de la comisión de dos o más infracciones muy graves en el plazo de tres años. Por lo que respecta al artículo 22.3 ALSEC, cambia con respecto al artículo 32.2 LFE, que preveía una posible publicación (teniendo en cuenta la repercusión social de la infracción cometida, el número de usuarios afectados y la gravedad del ilícito) de la resolución sancionadora en caso de infracciones graves y muy graves en el BOE y en dos periódicos de difusión nacional o en la página web del PSSIic y, en su caso, en el sitio de Internet del Ministerio; ahora, ya no es posible, sino preceptiva, la publicación de las resoluciones sancionadoras por la comisión de infracciones graves o muy graves, que serán publicadas, sin embargo, solamente en el sitio de Internet del Ministerio, indicando, en su caso, los recursos interpuestos contra ellas.

(40) Con el ALSEC, se mantienen las mismas circunstancias de la LFE y se incorporan algunas nuevas.

(41) Con el ALSEC, desparece el contenido del equivalente artículo 36.1.2º y 36.2 LFE.

(42) El artículo 11.1 ALSEC incorpora un apartado primero no contemplado en el artículo 18 LFE. El artículo 11.3.b) ALSEC prevé, al igual que el artículo 20.2 LFE, la constitución de un seguro de responsabilidad civil que, no obstante, ve ahora disminuido su importe de 3.000.000,00€ a 1.500.000,00€; sin embargo, si se presta más de un SSIisc (cualificado o no), en la nueva norma se prevé un incremento, no contemplado en la LFE, de 500.000,00€ por cada SSIisc (cualificado o no) adicional prestado.

(43) El artículo 9 ALSEC no exime al PSSIisc que expide el DNIe de constituir la garantía a la que están obligados todos los demás PSSIisc, como sí hacía el artículo 16.1, in fine, LFE. Tampoco incluye el artículo 9 ALSEC la previsión contenida en el artículo 16.2 LFE.

(44) El ALSEC contempla la posibilidad de practicar prueba de los documentos electrónicos, aun cuando no lleven incorporado servicio de confianza alguno, a diferencia de la LFE y en línea con el artículo 24 LSSICE, este último para una modalidad concreta de documento electrónico, cual es el contrato electrónico, si bien, mientras que este prevé (artículo 24.2 LSSICE) su naturaleza como prueba documental, el artículo 3.1 ALSEC, al regular la naturaleza probatoria de los documentos electrónicos en general, se remite a la LECiv., que los somete a las reglas de la sana crítica en su valoración como instrumentos electrónicos. Por lo demás, el artículo 3.1 ALSEC contempla la posibilidad de practicar prueba de los documentos electrónicos no sólo para probar su autenticidad (como el artículo 3.8 LFE), sino también su integridad, precisión de fecha y hora u otras características del mismo. Asimismo, la LFE establece que las costas, gastos y derechos que originen las comprobaciones de estos extremos serán a cargo de quien formule la impugnación, sin contemplar otra posibilidad, como es que la prueba se realice por la parte a quien interese su eficacia, como sí hace el artículo 3.1 ALSEC, que establece que, si la prueba requiere de un informe pericial *ad hoc* y en el documento se hubiera utilizado algún SSIisc cualificado y previsto en el RIE-SCTE (hecho que, por sí sólo, sin informe, otorga la presunción de que el documento electrónico reúne la característica cuestionada y que el SSIisc se ha prestado correctamente si figuraba, en el momento relevante a los efectos de la discrepancia, en la lista de PSSIisc), estos gastos serán a cuenta de la parte que solicitó dicho informe (sea la parte que pone en duda el documento electrónico o la parte a quien interesa su eficacia), mientras que, si no se hubiera utilizado ninguno de estos SSIisc, la parte a quien beneficie el documento electrónico deberá correr con los gastos del informe pericial que, en su caso, se solicitara. Por último, el artículo 3.2 ALSEC introduce una previsión no contemplada hasta ahora en la LFE, como es la regulación de los SSIisc contratados o los certificados emitidos como cualificados tras la pérdida de cualificación de un PSSIisc o de un concreto SSIisc.

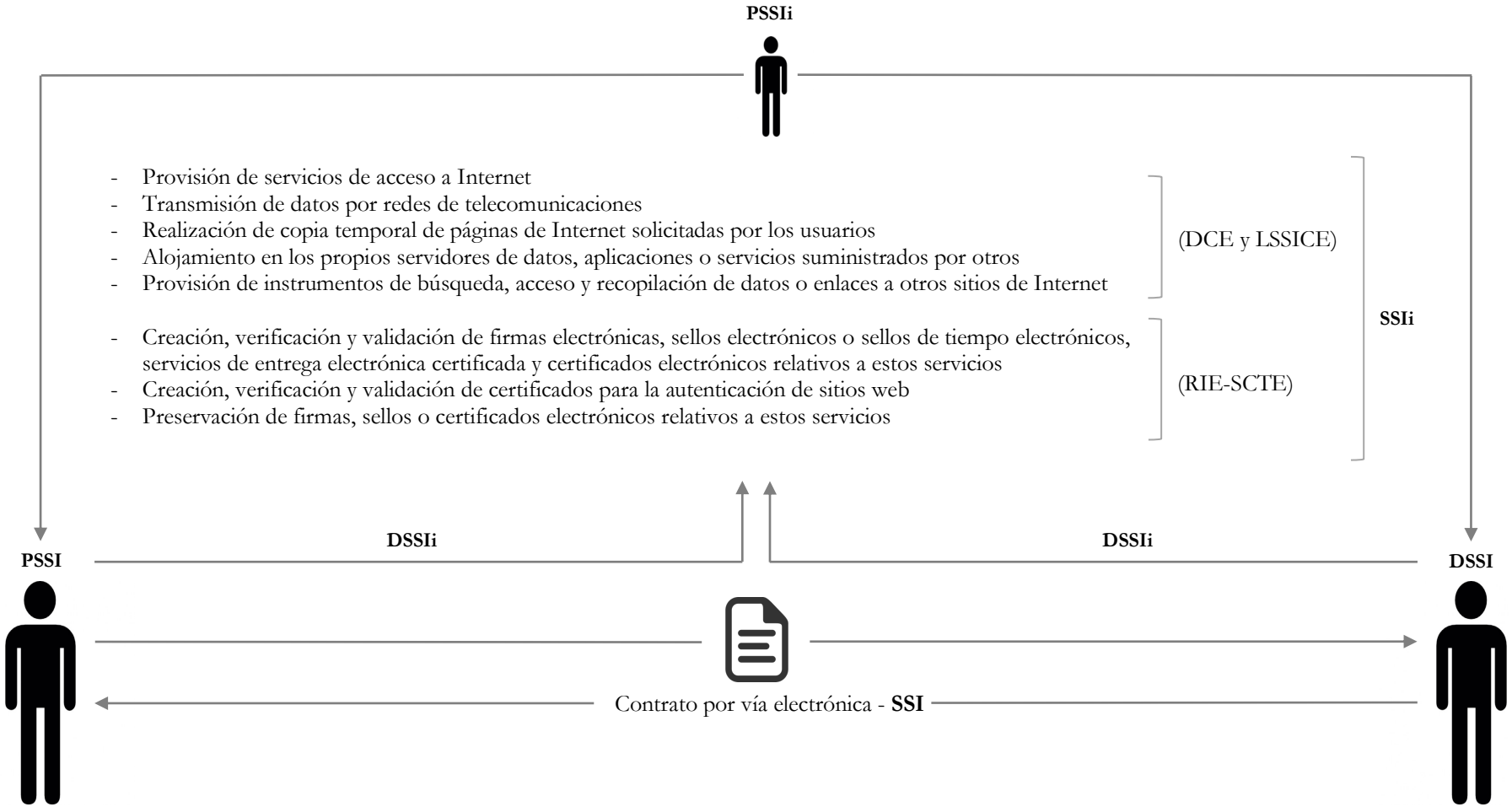
(45) El artículo 30.2, ab initio, LFE, contemplaba toda la información que los PSSIic debían comunicar al inicio de su actividad. Este deber de comunicación no se contempla en el RIE-SCTE ni en el equivalente artículo 20.2 ALSEC.

(46) La LFE contemplaba una D. T. 2ª para los PSSIic en general, mientras que el ALSEC lo hace sólo para los PSSIisc no cualificados. Además, varía el plazo de la comunicación, que pasará de un mes desde la entrada en vigor de la norma a tres meses desde dicha entrada en vigor.

(47) Desaparece en el ALSEC, con respecto a la LFE, el fundamento constitucional 18º del artículo 149 CE.

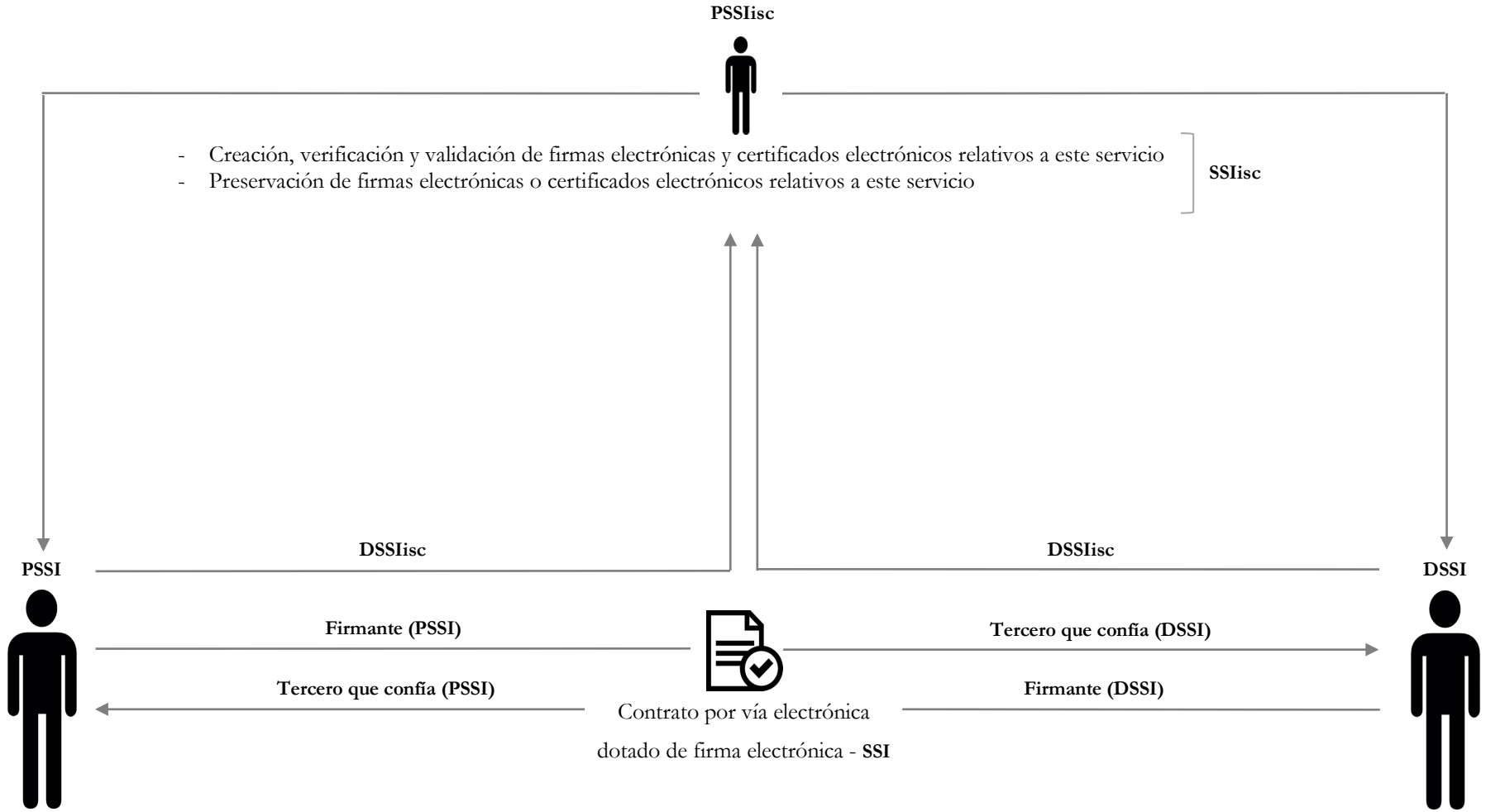
(48) Estos apartados sólo son aplicables a los PSSIisc de firma electrónica cualificada.

## Anexo XVI. Dinámica del contrato electrónico como servicio de la sociedad de la información



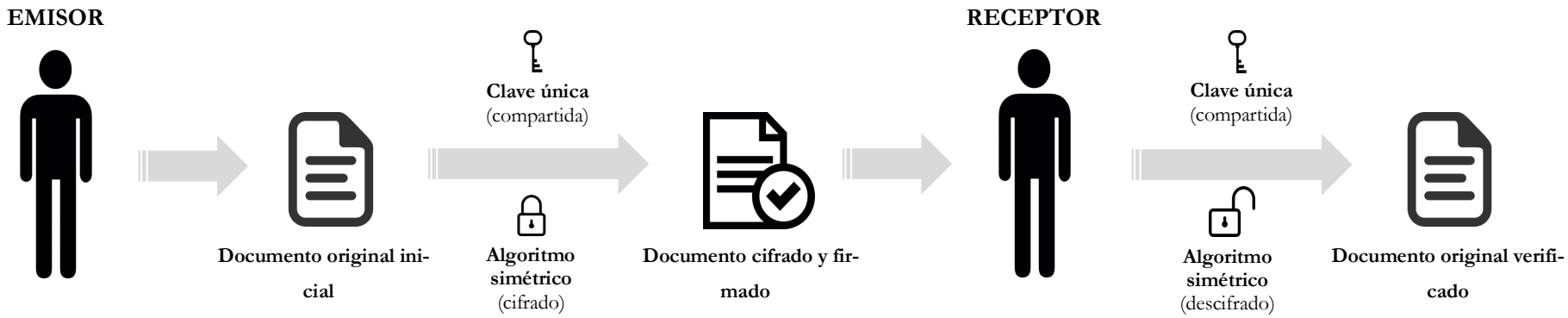

*Anexo XVI. Dinámica del contrato electrónico como servicio de la sociedad de la información. Fuente: elaboración propia*

Anexo XVII. Dinámica del contrato electrónico dotado de firma electrónica como servicio de la sociedad de la información



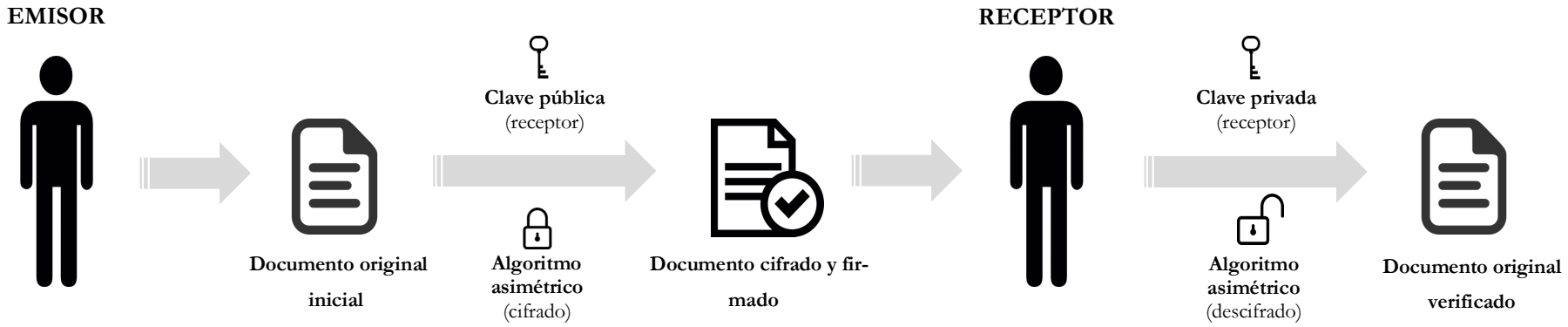

*Anexo XVII. Dinámica del contrato electrónico dotado de firma como concreto servicio de la sociedad de la información. Fuente: elaboración propia*

Anexo XVIII. Esquema del cifrado de clave simétrica



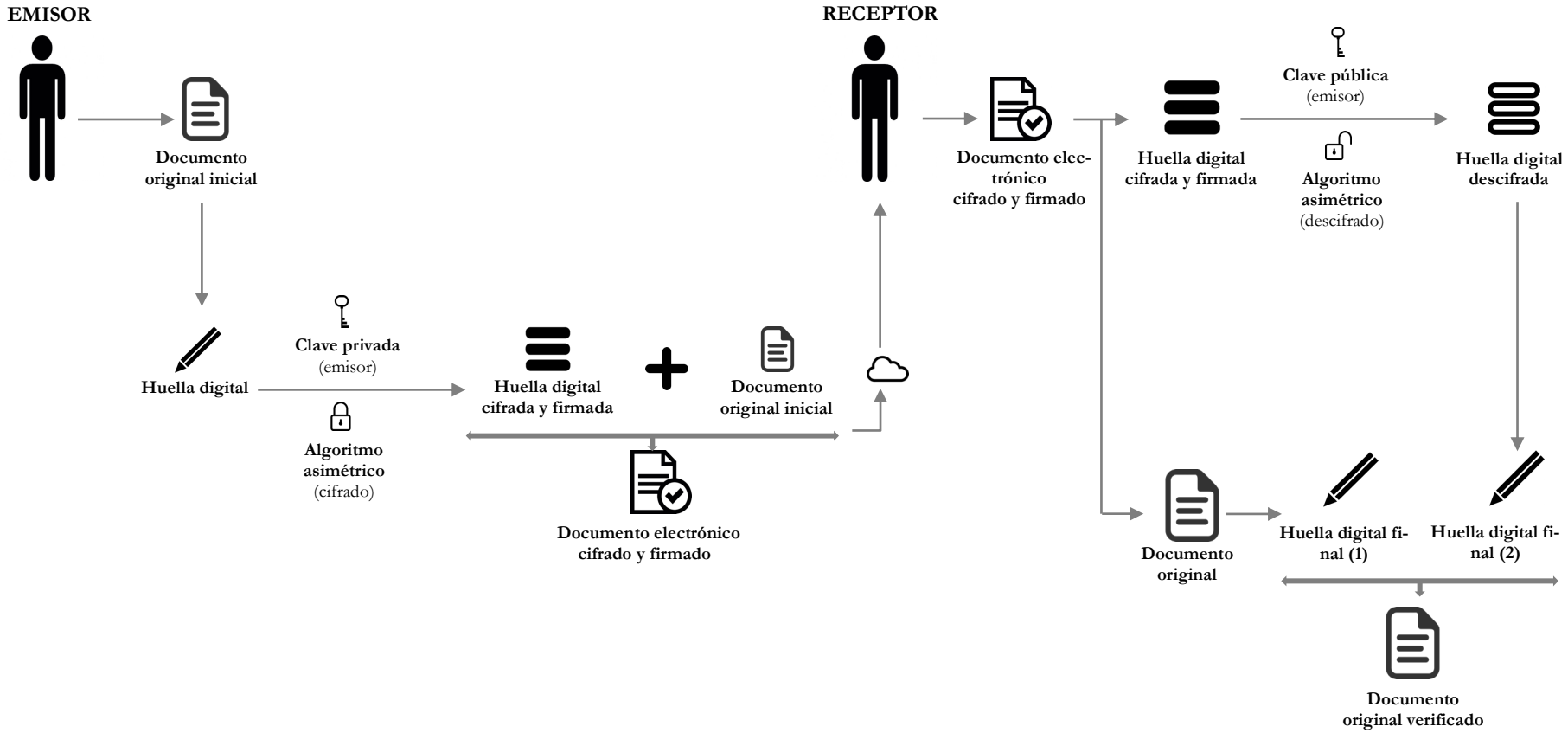

*Anexo XVIII. Esquema del cifrado de clave simétrica. Fuente: elaboración propia*

Anexo XIX. Esquema del cifrado de clave asimétrica pública del receptor



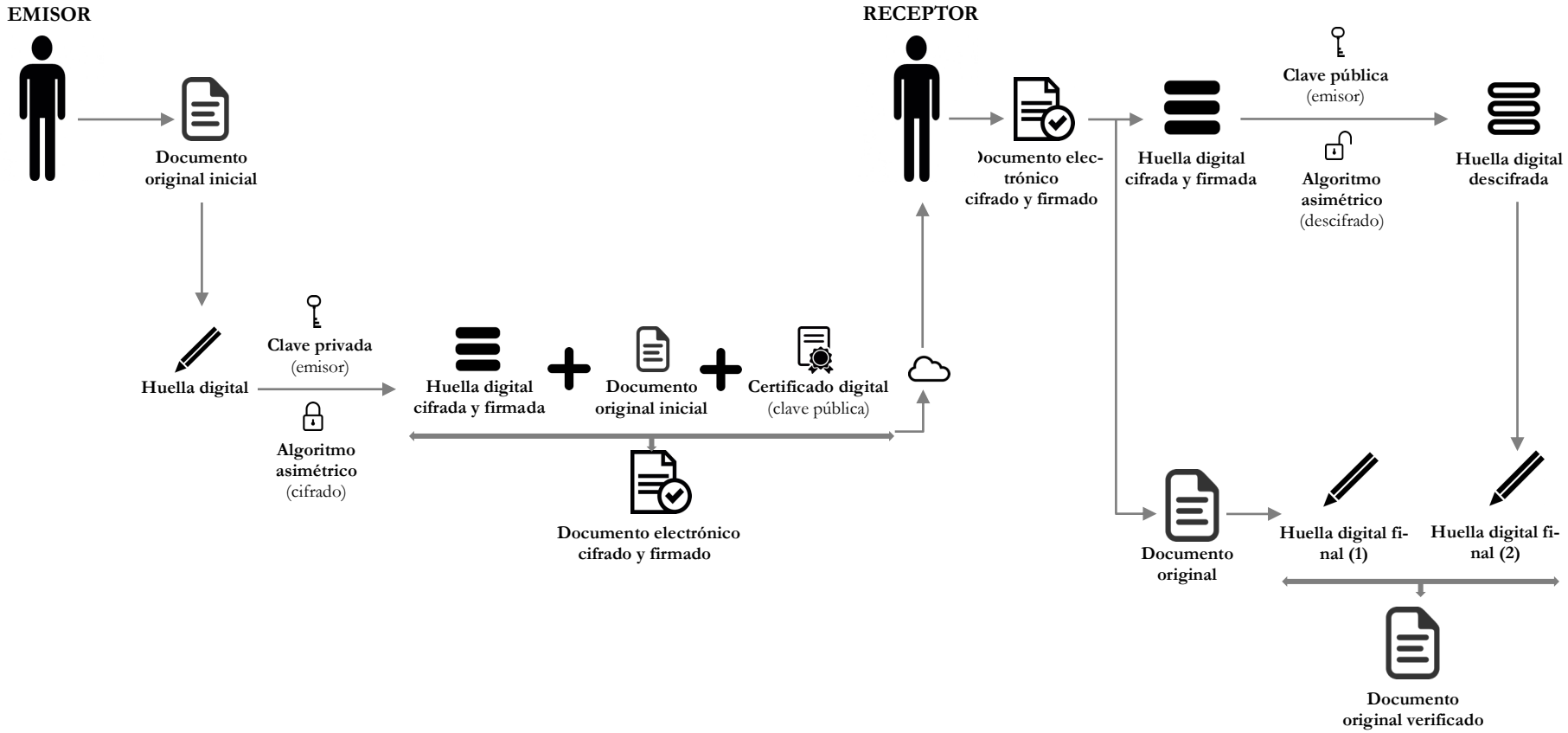

*Anexo XIX. Esquema del cifrado de clave asimétrica pública del receptor. Fuente: elaboración propia*

Anexo XX. Esquema del cifrado de clave asimétrica pública del emisor: la firma digital



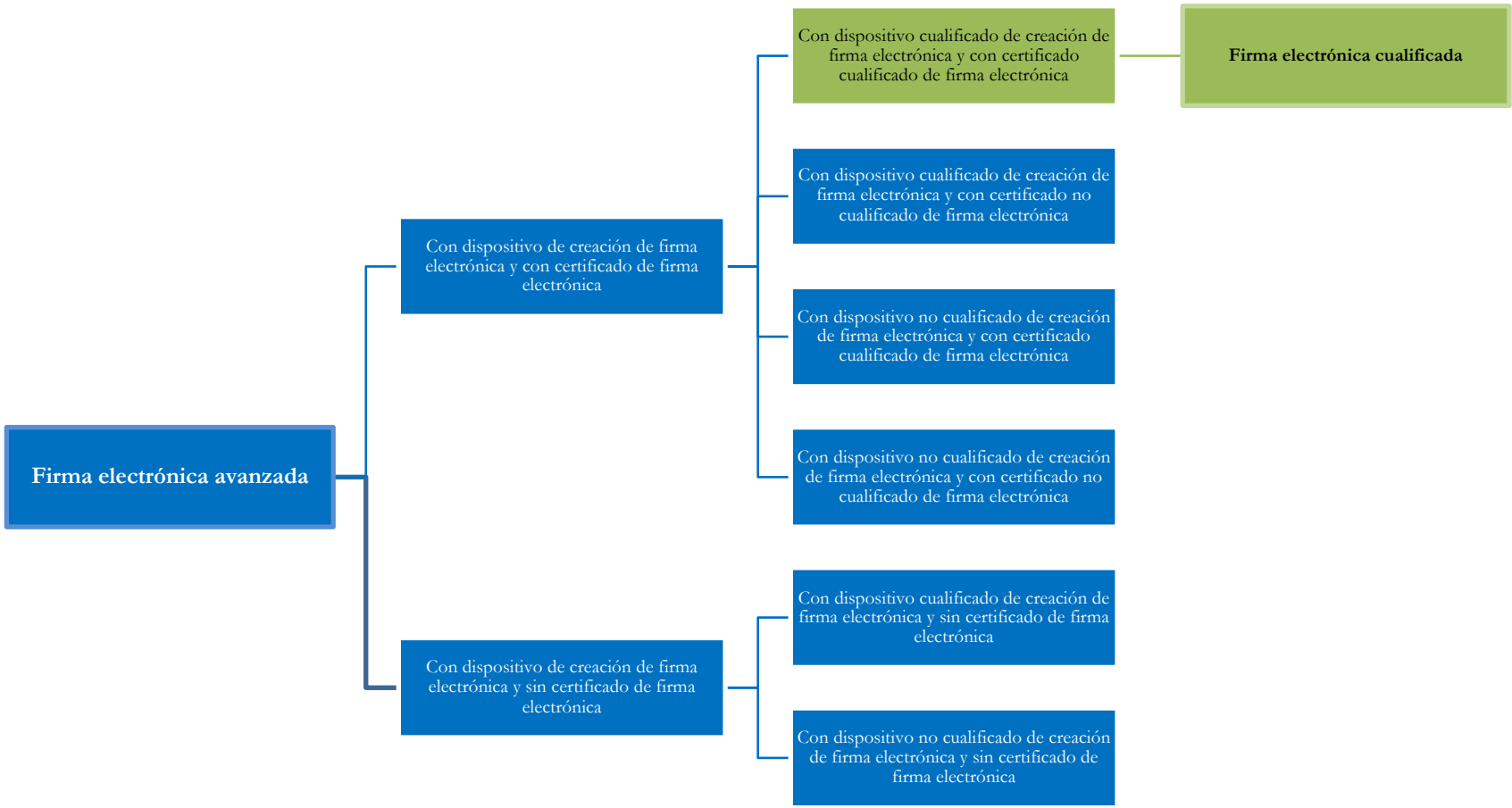

*Anexo XX. Esquema del cifrado de clave asimétrica pública del emisor: la firma digital. Fuente: elaboración propia*

Anexo XXI. Esquema de la firma digital dotada de certificado electrónico



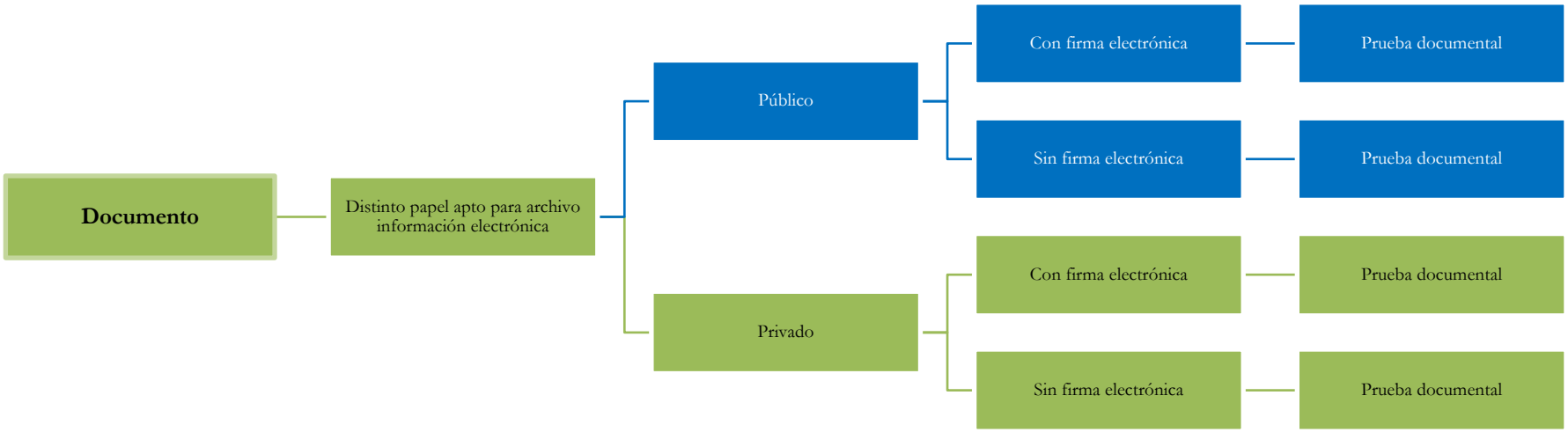

*Anexo XXI. Esquema de la firma digital dotada de certificado electrónico. Fuente: elaboración propia*

# Anexo XXII. Posibilidades en materia de firma electrónica



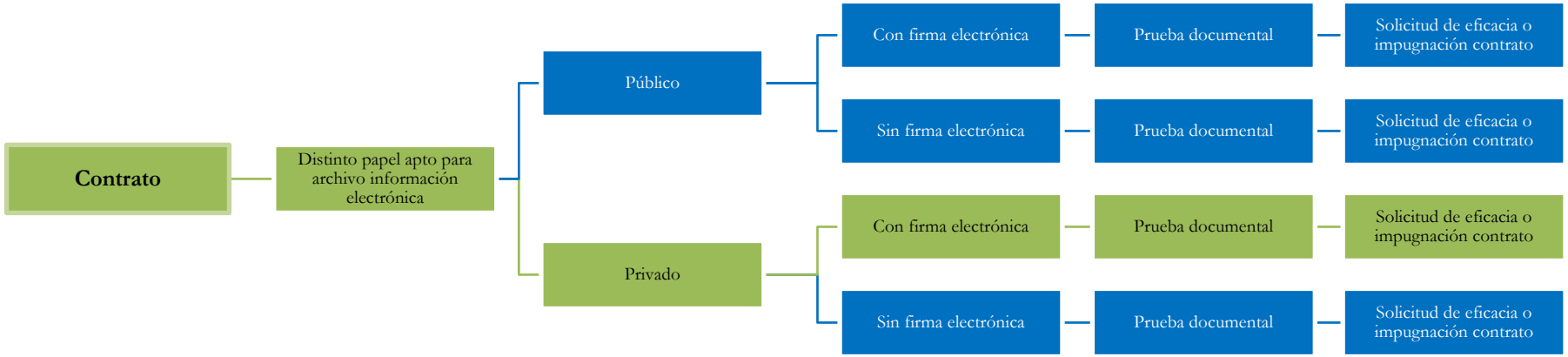

*Anexo XXII. Posibilidades en materia de firma electrónica. Fuente: elaboración propia*

# Anexo XXIII. Valor probatorio del documento electrónico



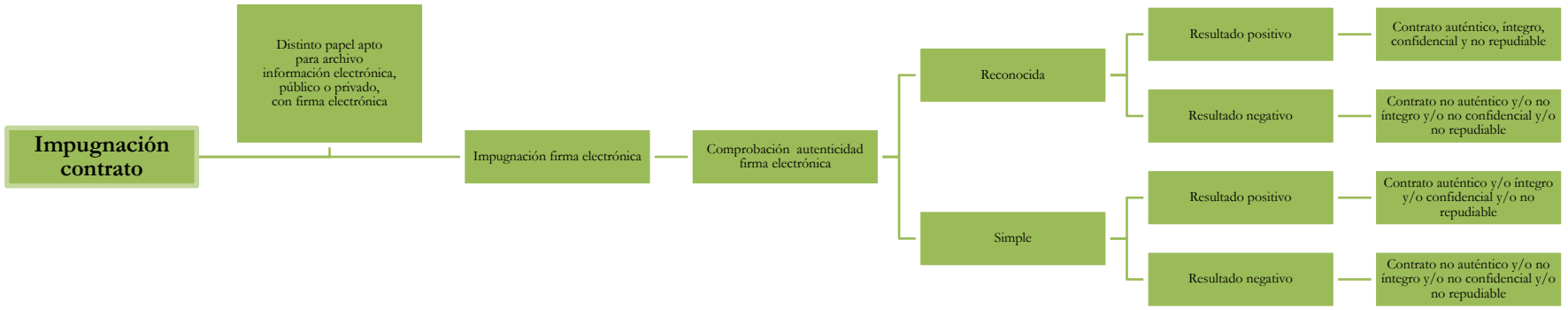

*Anexo XXIII. Valor probatorio del documento electrónico (en verde aparece la línea argumental seguida en el presente estudio). Fuente: elaboración propia*

Anexo XXIV. Solicitud de eficacia o impugnación de un contrato electrónico acompañado de firma electrónica



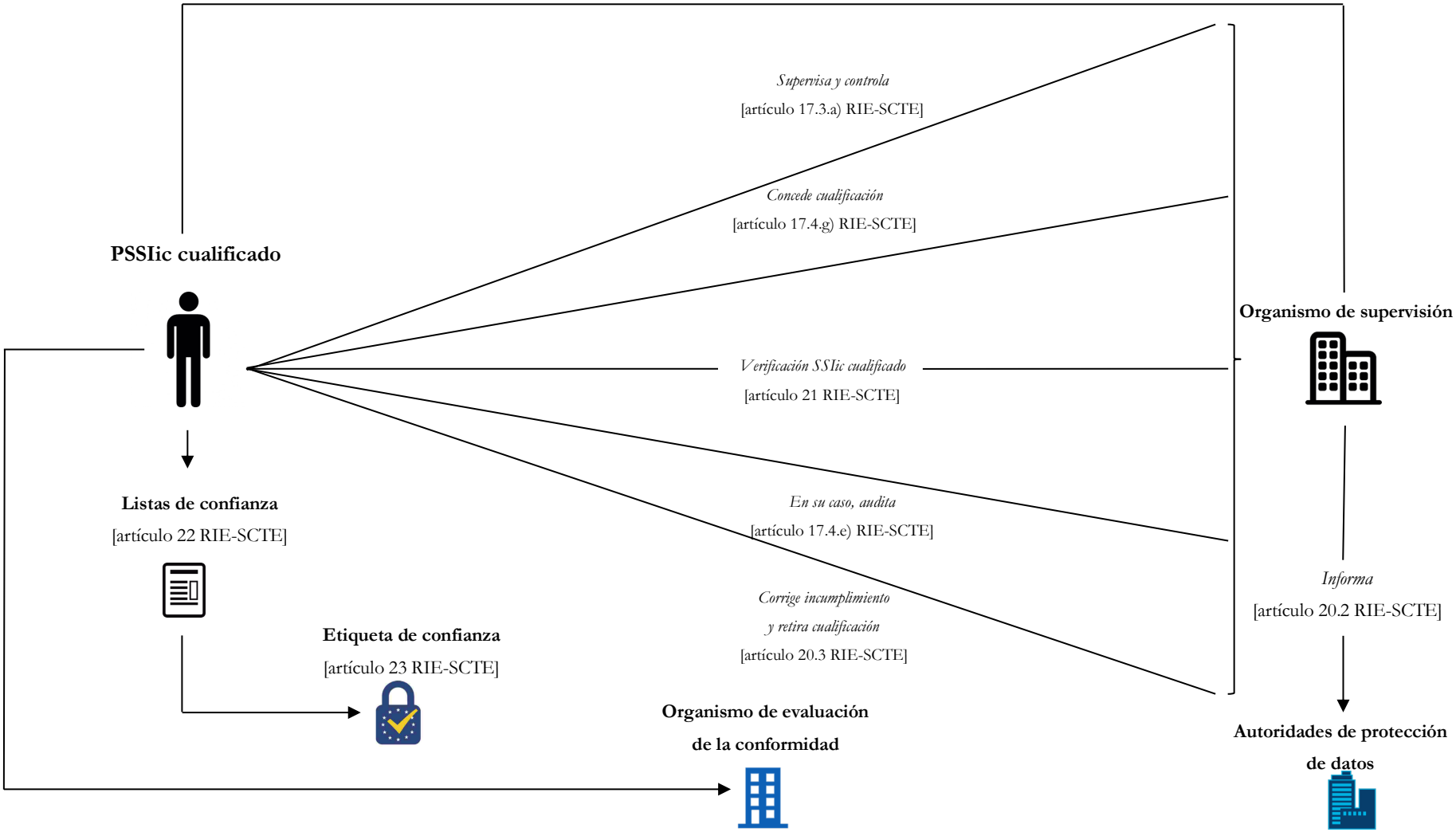

*Anexo XXIV. Solicitud de eficacia o impugnación de un contrato como documento acompañado de firma electrónica (en verde aparece la línea argumental seguida en el presente estudio). Fuente: elaboración propia*

## Anexo XXV. Impugnación de la firma electrónica acompañada a un contrato electrónico



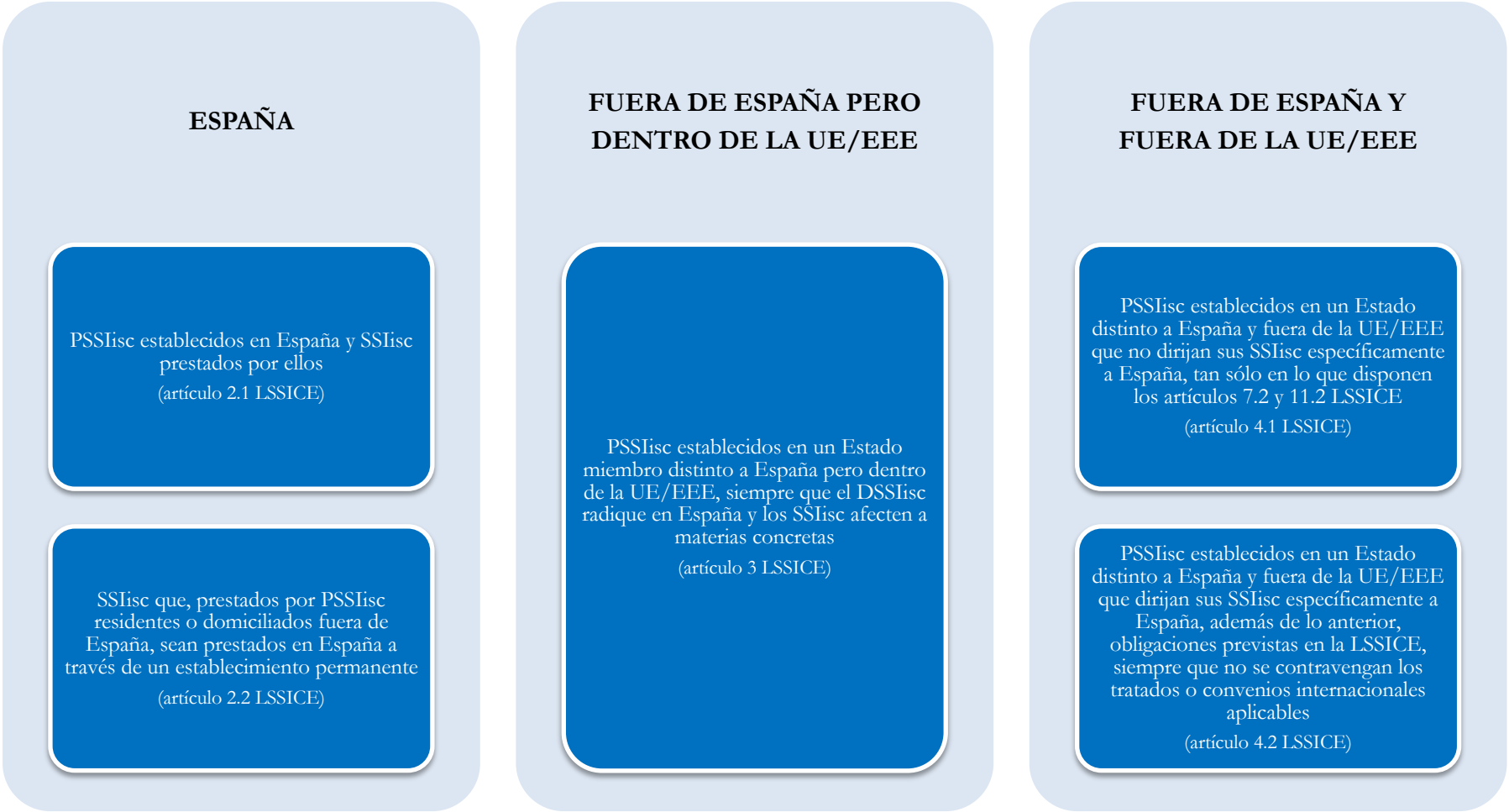

*Anexo XXV. Impugnación de la firma electrónica acompañada a un contrato electrónico (en verde aparece la línea argumental seguida en el presente estudio). Fuente: elaboración propia*

## Anexo XXVI. Estructura de funcionamiento de los PSSIisc cualificados



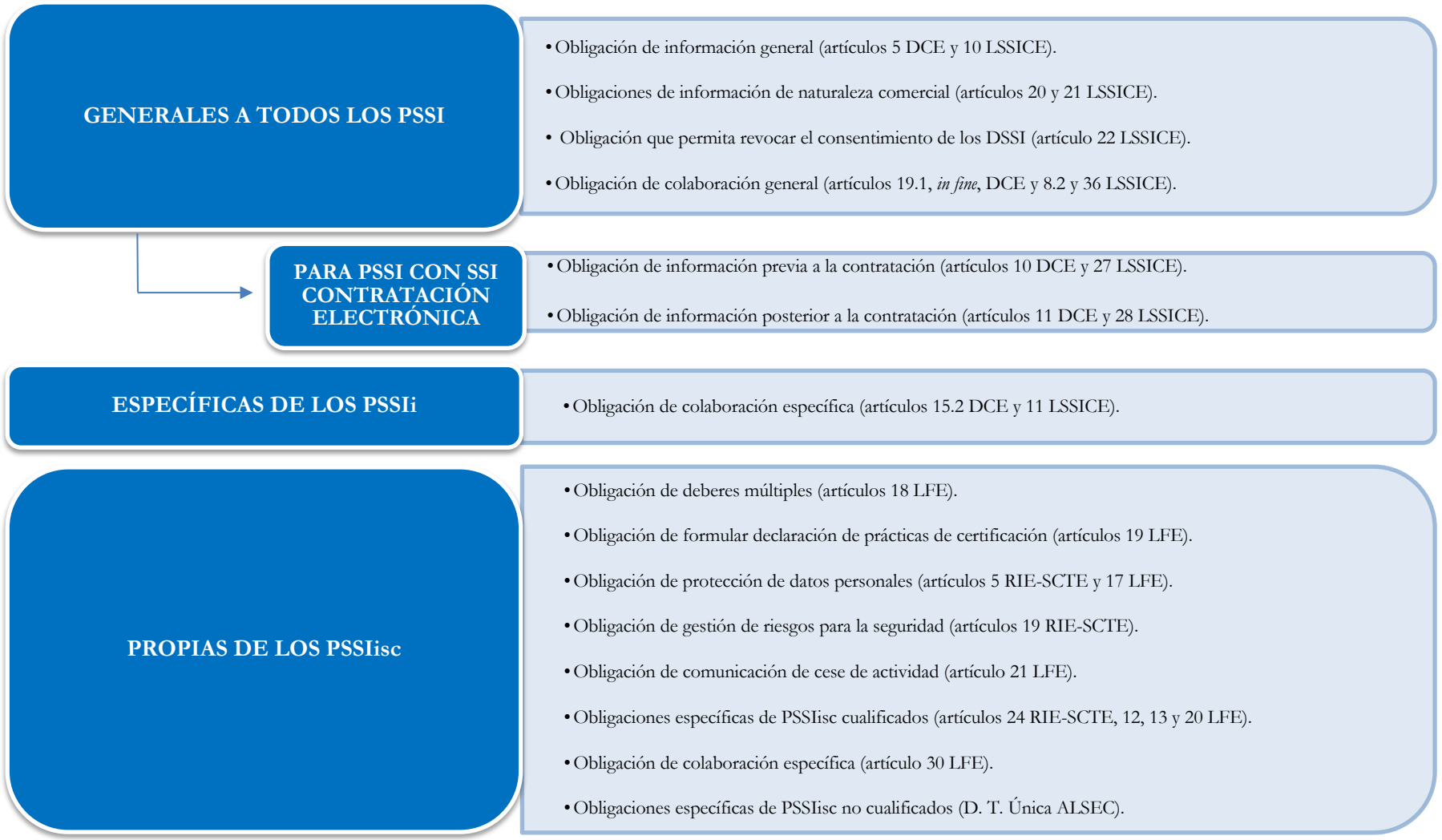

*Anexo XXVI. Estructura de funcionamiento de los PSSIisc cualificados. Fuente: elaboración propia*

Anexo XXVII. Ámbito de aplicación de los PSSIisc



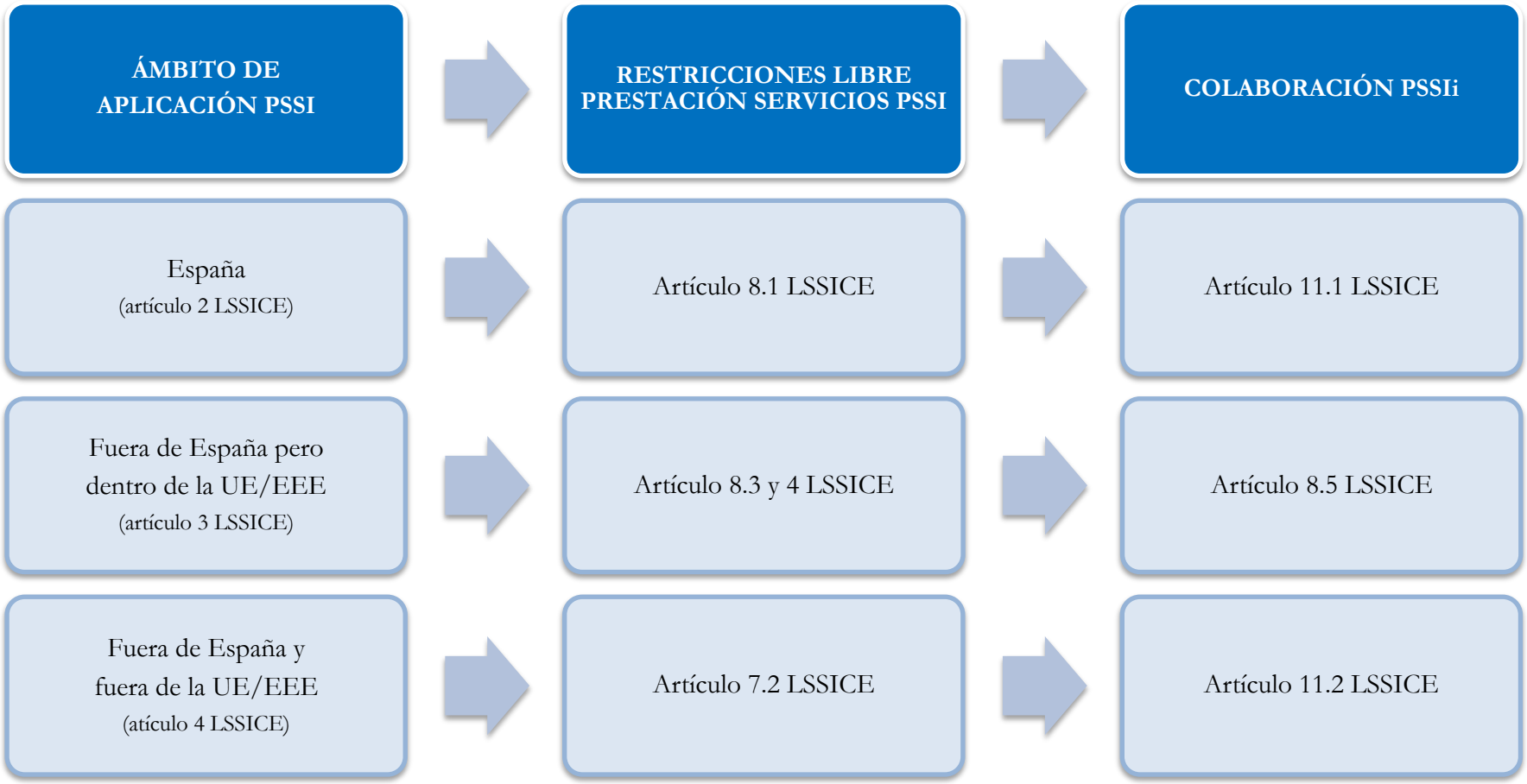

*Anexo XXVII. Ámbito de aplicación de los PSSIisc. Fuente: elaboración propia*

## Anexo XXVIII. Obligaciones actuales de los PSSIisc



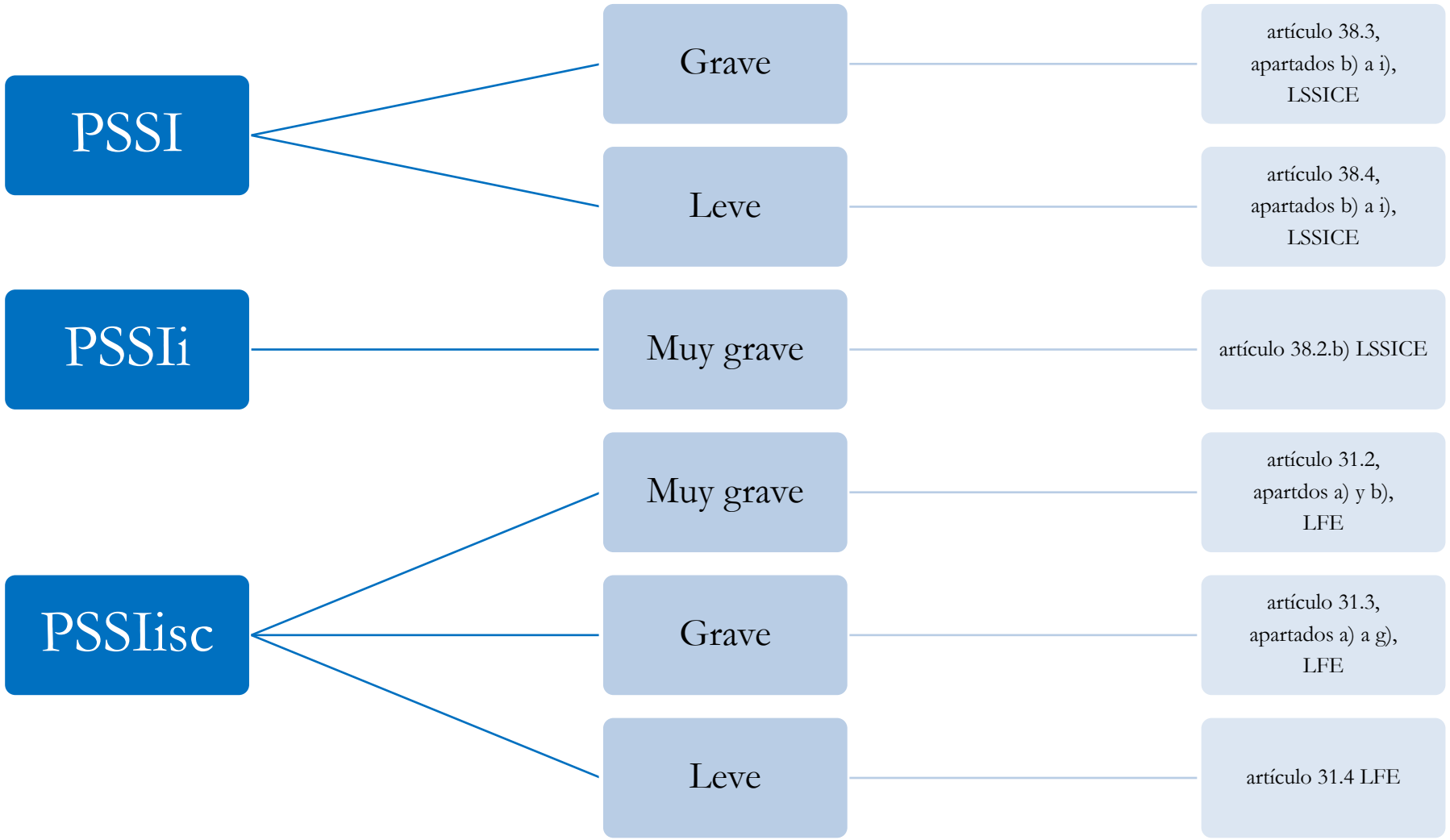

*Anexo XXVIII. Obligaciones de los PSSIisc. Fuente: elaboración propia*

Anexo XXIX. Ámbito de aplicación, restricciones de los PSSI y colaboración de los PSSIi




*Anexo XXIX. Ámbito de aplicación y restricciones de los PSSI y colaboración de los PSSIi. Fuente: elaboración propia*

Anexo XXX. Posibles infracciones de los PSSIisc




*Anexo XXX. Posibles infracciones de los PSSIisc. Fuente: elaboración propia*